FLUKE networks

AirCheck™
Wi-Fi Tester

Getting Started Guide

Guide d'introduction

Erste Schritte

Guia de Introdução

Руководство по началу работы с устройством

Guía de funcionamiento básico

スタート・ガイド

入门指南

사용 시작 안내서

PN 3434814 12/2009 Rev. 4, 8/13
©2009-2013 Fluke Corporation. Printed in USA.
All product names are trademarks of their respective companies.
Wi-Fi® is a registered trademark of the Wi-Fi Alliance.

FLUKE networks

AirCheck™
Wi-Fi Tester

Getting Started Guide

PN 3434814 12/2009 Rev. 4, 8/13
©2009-2013 Fluke Corporation. Printed in USA.
All product names are trademarks of their respective companies.
Wi-Fi® is a registered trademark of the Wi-Fi Alliance.

LIMITED WARRANTY AND LIMITATION OF LIABILITY

Fluke Networks guarantees this product to be free from defects in material and workmanship for one year from the date of purchase. Parts, accessories, product repairs and services are warranted for 90 days, unless otherwise stated. Ni-Cad, Ni-MH and Li-Ion batteries, cables or other peripherals are all considered parts or accessories.

This warranty does not cover damage from accident, neglect, misuse, alteration, contamination, or abnormal conditions of operation or handling. Resellers are not authorized to extend any other warranty on Fluke Networks' behalf.

To obtain service during the warranty period, contact your nearest Fluke Networks authorized service center to obtain return authorization information, then send your defective product to that Service Center with a description of the problem.

THIS WARRANTY IS YOUR ONLY REMEDY. NO OTHER WARRANTIES, SUCH AS FITNESS FOR A PARTICULAR PURPOSE, ARE EXPRESSED OR IMPLIED. FLUKE NETWORKS IS NOT LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOSSES, ARISING FROM ANY CAUSE OR THEORY.

Since some states or countries do not allow the exclusion or limitation of an implied warranty or of incidental or consequential damages, this limitation of liability may not apply to you.

4/04

Fluke Networks
PO Box 777
Everett, WA 98206-0777
USA

Contents

Accessing the Users Manual 1
Warning Information 2
General Specifications 5
Maintenance, Service, and Equipment Protection Impairment 6
Contact Fluke Networks 7
Battery Charging and Life 8
Home Screen 9
Minimum Configuration for the Best Performance 12
What You Can Learn About Your Wireless Network? 13
What is the Health of My Network? 13
What is in the Wireless LAN? 16
Can Devices Connect to the Wireless Network? 18
What Causes Slow Network Performance or Dropped Connections? 19
Are There Security Risks in the Network? 20
How Can I Locate an Access Point? 22
How Can I Document My Network and My Test Session? 23
How Can I Erase Everything on my AirCheck? 23
Discover Channels, Networks, APs, or Clients 24

Accessing the Users Manual

This guide provides basic information to help you get started using the AirCheck™ Wi-Fi Tester. For additional information, see the users manual on the Product CD.

The CD also contains the AirCheck Manager application to assist you with getting the most out of your tester.

Warning Information

The AirCheck ™ Wi-Fi Tester is a dedicated, handheld tool for quickly verifying and troubleshooting Wi-Fi networks.

⚠Warning⚠

Read all safety information before you use the Product.

Use the Product only as specified, or the protection supplied by the Product can be compromised.

Carefully read all instructions.

Use only Fluke approved power adapters to charge the battery.

Do not use the Product around explosive gas, vapor, or in damp or wet environments.

Examine the case before you use the Product. Look for cracks or missing plastic. Carefully look at the insulation around the terminals.

Batteries contain hazardous chemicals that can cause burns or explode. If exposure to chemicals occurs, clean with water and get medical aid.

Remove the batteries if the Product is not used for an extended period of time, or if stored in temperatures above 50 °C. If the batteries are not removed, battery leakage can damage the Product.

Do not short the battery terminals together.

Do not disassemble or crush battery cells and battery packs.

Do not put battery cells and battery packs near heat or fire. Do not put in sunlight.

Do not continuously charge battery packs when not in use.

Do not expose battery pack to mechanical shock.

Do not open the battery pack. There are no user serviceable parts inside.

Refer to the Product manual for proper instructions on charging the battery pack

To prevent possible fire, electric shock, personal injury, damage to equipment, or inaccurate test results, read the safety information in the *AirCheck Users Manual* before using the tester.

	Warning or Caution: risk of damage to or destruction of equipment or software. See explanations in manual.
	Warning: Risk of electrical shock.

	Do not put products that contain circuit boards into waste containers. Refer to local regulations for disposal procedures.
	This equipment contains a Class 2 radio.
	Conforms to relevant European Union directives.
	Conforms to FCC Rules, Parts 15.107, 15.109.
	Listed by the Canadian Standards Association.
	Conforms to relevant Australian standards
	Conforms to relevant South Korean EMC Standards.

Additional South Korean EMC Standard Information:

A급 기기 (업무용 방송통신기자재)	**이 기기는 업무용 (A 급) 전자파 적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며 , 가정 외의 지역에서 사용하는 것을 목적으로 합니다 .**
Electromagnetic Compatibility. Applies to use in Korea only. Class A Equipment (Industrial Broadcasting & Communications Equipment) [1]	[1] This product meets requirements for industrial (Class A) electromagnetic wave equipment and the seller or user should take notice of it. This equipment is intended for use in business environments and is not to be used in homes.

General Specifications

Battery Type: Removable, rechargeable lithium-ion battery pack (18.5 Watt-hrs)

Operating temperature and relative humidity: 32°F to 113°F (0°C to +45°C)

Operating relative humidity: (% RH without condensation) 90% (50°F to 95°F; 10°C to 35°C)75% (95°F to 113°F; 35°C to 45°C)

Storage: -4°F to 140°F (-20°C to +60°C)

Shock and vibration: Random, 2 g, 5 Hz-500 Hz (Class 2) 1 m drop test

Altitude: 4,000 m; Storage: 12,000 m

Safety: IEC/EN 61010-1: Cat none, Pollution degree 2

Maintenance, Service, and Equipment Protection Impairment

- The battery is the only user serviceable component. Do not open the case except to replace the battery.
- Use only replacement parts that are approved by Fluke Networks.
- If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment can possibly be impaired.
- To clean the case, use a soft cloth that is moist with water or water and a mild detergent.

Contact Fluke Networks

www.flukenetworks.com

support@flukenetworks.com

+1-425-446-4519

- Australia: 61 (2) 8850-3333 or 61 (3) 9329 0244
- Beijing: 86 (10) 6512-3435
- Brazil: 11 3759 7600
- Canada: 1-800-363-5853
- Europe: +31-(0) 40 2675 600
- Hong Kong: 852 2721-3228
- Japan: 03-6714-3117
- Korea: 82 2 539-6311
- Singapore: +65-6799-5566
- Taiwan: (886) 2-227-83199
- USA: 1-800-283-5853

Visit our website for a complete list of phone numbers.

Battery Charging and Life

Charge the battery for 4 hours before you use it for the first time. To charge the battery, connect the ac adapter to the battery connector on the AirCheck tester.

The battery life is approximately 5.5 hours during typical operation.

Shows the battery status. When the battery charge is low, the icon blinks.

Shows that the ac adapter is connected.

Home Screen

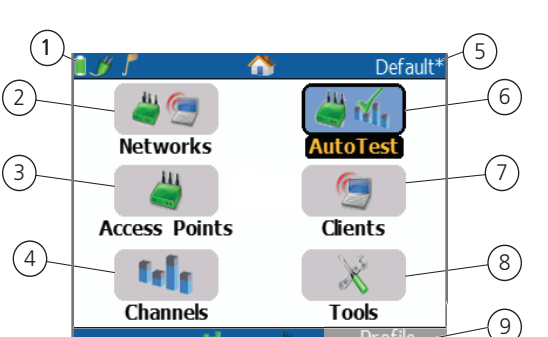


Figure 1. Home Screen Components

①

Shows the battery status. When the battery charge is low, the icon blinks. Connect the ac adapter to charge the battery and to make sure the tester continues to operate.

Shows that the ac adapter is connected.

Shows that the external antenna is connected.

Note

AirCheck will not transmit or connect to an access point when the external antenna is connected.

② **Networks**: Discovers wireless LANs.

③ **Access Points**: Discovers access points.

④ **Channels**: Shows usage of WLAN channels.

⑤ The name of the profile the tester is currently using. The profile is **Default** if you have not loaded a different profile. The name shows an asterisk if you have changed a setting on the tester since you loaded or saved the profile.

⑥ **AutoTest:** Automatically checks the health of your network by looking at air quality (channel usage and interference), network quality (network coverage and connectivity), and the presence of ad hoc networks. Rogue access point detection is optional and requires ACL configuration.

⑦ **Clients:** Discovers clients using your networks.

⑧ **Tools**: Lets you manage files and settings.

⑨ **Profile:** Shows a list of available profiles.

⑩ Left: The channel the tester is currently monitoring. The color of the bars shows the status of the country code for the regulatory domain. A red icon can indicate the operation of an illegal channel for the current country setting and/or the receipt of a different country code.

Right: The number of physical access points heard by the tester.

Up to 500 access points can be stored in the access point database on the tester. When the access point icon turns yellow, it indicates that greater than or equal to 400 access points have been discovered.

When the icon turns red, it indicates that 500 or more access points have been discovered and the access point database is full. Any new discovered access points will not be included in the list.

Minimum Configuration for the Best Performance

To change the language and country settings

1 Select **Tools**.

2 To change the language for the screens, select **Set language**. Highlight a language, then press F2 **Save**.

3 To change the country, select **Set country**, select the country where you will use the tester, then press F2 **Save**.

To get the best performance from your tester, use AirCheck™ Manager software to configure a profile and upload it to the tester. A profile can also be configured on the AirCheck tester and contains data that lets the tester do these tasks:

- Connect to networks that require security credentials.
- Show the correct authorization status for each access point. This lets you quickly see which access points are authorized parts of the network.
- Ping key network devices.
- Run a TCP Port Connect Test, using a hostname or an IP address and a designated port number.

What You Can Learn About Your Wireless Network?

What is the Health of My Network?

- **How is my Wi-Fi Air Quality?**
  Are my channels overloaded with access points and Wi-Fi traffic?
  Are any of my channels too noisy?

  Select **AutoTest**. After the AutoTest has run, select **Air Quality** to view the results of 802.11 Channel Utilization, Non-802.11 Channel Utilization, and Co-Channel Interference health assessment.

  The 802.11 Channel Utilization results include the top three busiest channels having the most Wi-Fi traffic. The channel utilization value along with the rating of ✓ Pass, ⚠ Warning, or ✗ Fail, is displayed. The test grade is based on a comparison of the actual value to user settable thresholds. These thresholds are configured in the **Tools > Thresholds / AutoTest Settings**.

  The Non-802.11 Channel Utilization results include the top three channels with the most non- 802.11 interference and noise. The channel utilization value along with the rating of ✓ Pass, ⚠ Warning, or ✗ Fail, is displayed.

  The Co-Channel Interference results include the top three channels with the most APs with a minimum signal strength and signal quality. The AP count along with the rating at or above of ✓ Pass, ⚠ Warning, or ✗ Fail, is displayed.

- **How is my Wi-Fi Network Quality?**
  Can I hear any access points that support my networks?
  Are there coverage holes in this area?
  Are there too many close APs using the same channel making my network slow?
  Can I connect?

  Select **AutoTest** - After the AutoTest has run, select **Network Quality** to view the results of Coverage, Co-Channel Interference, Security, and Connection health assessment.

  The Coverage results include the number of APs with good signal quality including both good signal strength and a good Signal to Noise Ratio supporting a network (SSID) along with the rating of ✓ Pass, ⚠ Warning, or ✗ Fail, is displayed. The test grade is based on a comparison of the actual values to user settable thresholds. The AP count and signal quality thresholds of signal level and signal-to-noise are set in the **Tools > Thresholds / AutoTest Settings > AP Coverage, Signal level** and **Signal-to-noise Threshold** screens.

  The Co-Channel Interference results include the number of overlapping APs for a network along with the rating of ✓ Pass, ⚠ Warning, or ✗ Fail, based on a single network comparison to thresholds. Thresholds for this test are set in the **Tools > Thresholds / AutoTest Settings > Network Quality co-channel thresholds** screen.

The Security results report whether all APs on the SSID use the same security credentials along with a rating of Pass, Warning, or Fail.

The Connection test attempts to connect to each network configured in your profile. Connection test results indicate whether you can connect to networks at your location or not with a test grade of Pass or Fail. Additional details about the connection e.g., channel, IP address received, connect rate is provided as a rating of Pass, Warning, or Fail.

- **What unauthorized or unknown access points are connected to my Wi-Fi network? Are they a security risk?**

  The Rogue Access Points test is an optional part of AutoTest, it indicates whether unauthorized or unknown access points are detected with a rating of Pass, Warning, or Fail. Results include a list of all rogue access points heard at your location. Identification of rogue access points requires configuration of an Access Control List (ACL). ACL configuration is available from the AutoTest screen by selecting **Rogue Access Points > ACL** or **Home> Access Points > ACL**.

What is in the Wireless LAN?

- ❑ **What wireless LANs are available?**

  Select **Networks** to see a list of wireless LANs and the access points that connect to each network. To see all access points that are available at your location, select **Access Points**.

- ❑ **What access points are available? Are the signal strengths sufficient?**

  Select **Access Points** to see a list of access points available at your location and the signal strength of the access points. To see bar graphs of the signal strength and noise for an access point, highlight the access point, then press SELECT.

- ❑ **Is the access point configured correctly?**

  From the home screen, select **Access Points**, highlight an access point, then press SELECT.

- ❑ **Are there new access points in the area? Are they your access points, your neighbors, or a rogue?**

Use the device authorization status (ACL) feature to automatically report when new access points are discovered at your location. To make use of this feature, configure access point authorization status for each access point (e.g. authorized or neighbor), next set the default authorization status to ? **Unknown**. As a result, the default authorization status of ? **Unknown** will be assigned to any access points not previously discovered. Lastly, select **Access Points** from the home screen to see any access points marked as ? **Unknown**.

Alternatively, save the test session which includes the list of discovered access points. Use AirCheck Manager to compare the access point list to a previously saved session file to see if additional access points have been discovered.

To specify a default device authorization of either unknown or authorized, select **Tools > Set Device Authorization (ACL) default**

- **What wireless clients use the network?**

  From the home screen, select **Clients**. You can also drill into AP or channel details to see the list of associated clients.

Can Devices Connect to the Wireless Network?

Use the tester to verify connectivity.

- ❑ **Can a device connect as a client to the network (SSID)?**

  Select **Networks**, highlight a network, then press F1 **Connect**.

  Note

  To connect to a secure network, the tester must have a profile that includes security credentials.

- ❑ **Can a device connect to an access point (BSSID)?**

  Select **Access Points**, highlight an access point, then press F1 **Connect**. If an ***** is on the right of **Connect**, this indicates security has not been configured on the tester for that network. Press **Connect*** and you are guided through entering the security settings. When done, it is saved to the current profile. Press **Tools**, then **Manage profiles / network passwords** to re-edit the security settings if needed.

- ❑ **If a device cannot connect to a network or access point, where does the connection procedure fail?**

  Look at the connection log. Press F2 **Log** from the **Connect to Network** or **Connect to Access Point** screen.

- ❑ **Can a device ping a network device?**

Do a ping test. Connect to a network or access point, then press F1 **Start tests**.

Note

*Ping targets can be added by selecting **Tools > Manage profiles / network passwords > Edit targets > Add**. You can add a target with an IP address or hostname (URL).*

*If an ***** is on the right of **Connect**, this indicates security has not been configured on the tester for that network. Press **Connect*** and you are guided through entering the security settings.*

- ❑ **Does the network interface card in a client operate correctly?**

  Select **Clients**, then look in the SSID column. Dashed SSIDs are probing clients and clients with an SSID name displayed are associated clients. Press SELECT and see if the client transmits probe request frames.

What Causes Slow Network Performance or Dropped Connections?

- ❑ **Is the signal strength sufficient?**

  Select **Access Points**. The **Access Points** screen shows the signal strength for each access point. Select an access point to see more details about the signal strength and congestion.

- ❑ **Is the network too busy?**

  Select **Channels** to see an overview of channel usage and the number of access points that use each channel. To see a graph, highlight a channel, then press SELECT.

- **Is there non-802.11 interference on a channel?**

  Select **Channels**. Non-802.11 interference is gray. This noise can interfere with WLAN connections or performance. Non-802.11 noise can come from microwave ovens, wireless telephones, Bluetooth® devices, motion detectors, wireless cameras and other wireless devices.

  Note

  *The previous three measurements are also summarized in the **AutoTest** feature.*

Are There Security Risks in the Network?

- **Do networks have the expected level of security?**

  Select **Networks**. Networks that have unsecured access points show a red lock ( ).

- **Are there any ad hoc networks in the area?**

  Select **Networks**. Stations that are operating in ad hoc network mode will be marked with the ad hoc icon ( ) in the SSID column. Ad hoc stations can be risks to network security or can violate network policies.

  AutoTest includes an Ad Hoc Network test that flags ad hoc stations.

- **Are there rogue access points in the area? Where are they?**

AirCheck can be used to help track the authorization status of discovered access points. By default, when access points are discovered, they are assigned an authorization status of ? **Unknown**. You may change the status of individual or groups of access points to reflect their relationship to your network e.g., authorized, neighbor, unauthorized.

You also have the option of changing the default device status from ? **Unknown** to ✓ **Authorized**. Once changed, all discovered access points will be identified as ✓ **Authorized**. You may then review the list and assign status to individual access points accordingly. For example, if you know that an access point is a rogue, you may give it the status of **Flagged device** or ⚠ **Unauthorized device**.

To specify a default device authorization, select **Tools > Set Device Authorization (ACL) default**.

To give an access point or a group of access points an authorization status, select **Access Points**, highlight an access point, then press F2 **ACL**.

You can set the authorization status for all access points to ✓ **Authorized** by selecting ✓ **Set All APs to Authorized**. This will cause all discovered access points to be marked as ✓ **Authorized**. Using this approach, when the default authorization status is then set to ? **Unknown**, newly discovered access points will be shown as ? **Unknown**. Overall, this method will provide quick visibility into security risks or new access points.

You can also set a series of APs to authorized or unauthorized based on the AP BSSID/MAC or a Vendor MAC prefix by selecting **Set AP series to Authorized** or **Set AP series to Unauthorized**. These options may save you configuration time and provide quick visibility into potential issues. For example, if a specific vendor's equipment is not allowed per your network policy, use the vendor MAC prefix to set the ACL to unauthorized. When those access points are detected, they will automatically be reported as unauthorized.

Note

When you save your profile, the assigned ACLs will also be saved as part of that profile.

AutoTest optionally includes a Rogue Access Point Test which detects and reports rogue access points. To enable this functionality, go to **Tools > Thresholds/AutoTest Settings > Rogue Access Point AutoTest**. For accurate and meaningful test results, you must configure access point ACLs prior to running AutoTest.

How Can I Locate an Access Point?

Select **Access Points**, select one access point, then press F2 **Locate** on the **Access Point Details** screen. You may also use the optional Fluke Networks external directional antenna to help you find access points faster.

How Can I Document My Network and My Test Session?

Save the session (press), then use AirCheck Manager software to download the data to a PC and make a report.

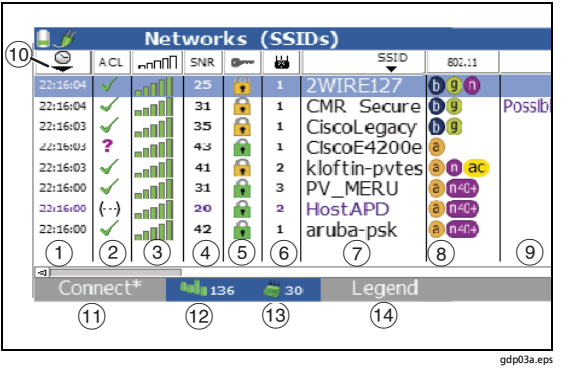
How Can I Erase Everything on my AirCheck?

If you want to erase all settings, session data and profiles from the tester, select **Tools > Erase All** - Everything that has been saved or stored on the AirCheck tester is erased.

Discover Channels, Networks, APs, or Clients

To discover channels, networks, access points, or clients, select **Channels**, **Networks, Access Points,** or **Clients** from the home screen. Figure 2 shows a **Networks** list.

To see details about a network or an access point, use ◁▲ ▼▷ to highlight the network or access point, then press SELECT.



gdp03a.eps

Figure 2. Networks List

① : The time when the tester first heard the network. To see networks that come into range as you move through an area, sort the list in descending sequence for the timestamp column.

Press , then move through an area. Networks that come into range are added to the top of the list. Networks that become out of range become gray if **Gray inaudible access points** is enabled.

② **ACL:** The authorization status of the access point. The default status is **? Unknown**, but can be changed to ✓ **Authorized**. Change the status of each access point to show how it is related to your network. To change the status, select **Access Points** from the home screen, select an access point, then press F2 **ACL**.

(...): All access points in the network do not have the same authorization status.

③ : The maximum signal strength of all the access points for a network SSID.

④ **SNR:** Signal to noise level is a measure of signal strength relative to noise. The ratio is measured in decibels (dB).

⑤ : The security status of the network:

Red open lock: The network does not have security enabled.

Note

Some networks with an open lock will allow you to connect the tester and perform measurements including running the Ping test, but may not allow a PC connecting to the same network to connect to the web without a user ID and password.

Yellow closed lock: One or more access points use WEP or Cisco LEAP security protocol. These are less secure than other protocols.

Green closed lock: All access points use security protocols that are more secure than WEP, for example, WPA or WPA2.

(...): All access points in the network do not use the same type of security. For example, one uses WEP and another uses WPA.

⑥ : The number of access points the tester hears at your location.

⑦ **SSID**: Service Set Identifier. The name of the wireless network.

: The network has ad hoc devices. These are devices that communicate directly with other devices, not through an access point. Ad hoc devices can give hackers access to data transmitted on the network. (Some IT policies for networks allow ad hoc devices.)

[Hidden]: The network does not broadcast its SSID.

⑧ **802.11**: The 802.11 standards that the access points in the network use:

802.11a: Uses the 5 GHz band.

802.11b: Uses the 2.4 GHz band.

802.11g: Uses the 2.4 GHz band.

802.11n: Uses the 2.4 GHz or 5 GHz band.

802.11ac: Uses the 5 GHz band.

Red bars: The tester received a country code that is different from the setting in **Tools** > **Set country**. To identify the network or access point that transmits the code, select **Networks** or **Access Points**, then look for the red bars in the **802.11** column.

n40+ n40–: One or more access points use a bonded channel. Access points that use the 802.11n standard can bond a channel with an extension channel above (n40+) or below it (n40–) to make one 40 MHz channel. This wider channel gives the network higher throughput.

(...): All access points in the network do not use the same 802.11 standard.

⑨ **Notes**: Press ▸ to scroll to the notes field. The tester adds notes automatically. Networks that have notes are shown in purple.

(...): The network has multiple notes. To see all the notes, highlight the network, then press SELECT twice to go to the **Access Point Details** screen.

⑩ : **Sort 1**, descending and ascending sequences.

: **Sort 2**, descending and ascending sequences.

To sort the list in ascending or descending sequence, use ▲▼ and ◀▶ to highlight a column heading, then press SELECT or F1 **Sort 1**. For example, to quickly find the access point that has the strongest signal, highlight ▁▃▅▇ at the top of the column, then press SELECT or F1 **Sort 1**. This puts the access point with the strongest signal at the top of the list.

To sort in a secondary sequence, highlight a different column heading, then press F2 **Sort 2**.

⑪ Press F1 **Connect** to connect to the highlighted network.

The connect button shows as **Connect*** (with an asterisk) if the tester cannot connect to the highlighted network. To configure the network's security settings, press F1 **Connect***.

Note

To connect to a secure network, the tester must have a profile that includes security credentials. Create or edit security credentials on the tester or with AirCheck Manager. When you press ***Connect**** *on the tester, it will guide you through the security configuration. You can also press* ***Tools****, then* ***Manage profiles / network passwords*** *to reconfigure the security settings. The* ***** *to the right of* ***Connect*** *indicates no security settings have been configured. Refer to the Users Manual for setting up security procedures using Connect.*

⑫ 40: The channel the tester currently monitors. The color of the bars shows the status of the country code for the regulatory domain.

⑬ : The number of access points the tester hears at your location. This number does not include virtual access points if **Group virtual access points** is selected.

⑭ To see descriptions of the icons on the **Networks** screen, press F2 **Legend**.

To see details about the access points in a network, use ▲ ▼ to highlight a network, then press SELECT.

FLUKE networks

AirCheck™
Testeur Wi-Fi

Guide d'introduction

PN 3434814 12/2009 Rev. 4, 8/13 (French)
©2009-2013 Fluke Corporation. Printed in USA.
All product names are trademarks of their respective companies.
Wi-Fi® is a registered trademark of the Wi-Fi Alliance.

EXCLUSION DE GARANTIE ET RESPONSABILITE LIMITEE

La société Fluke Networks garantit l'absence de vices de matériaux et de fabrication de ce produit pendant une période d'un an à compter de la date d'achat. Les pièces, accessoires, services de réparation ou d'entretien des produits sont garantis 90 jours sauf mention contraire. Les batteries Ni-Cad, Ni-MH et Li-Ion, les câbles et autres matériels périphériques font tous partie de la liste des pièces ou des accessoires.

Cette garantie ne s'applique pas aux produits mal utilisés, modifiés, négligés, endommagés par accident ou soumis à des conditions anormales d'utilisation et de manipulation. Les distributeurs agréés par Fluke Networks ne sont pas autorisés à appliquer une garantie plus étendue au nom de Fluke Networks.

Pour avoir recours au service de la garantie, contactez le centre de service Fluke Networks le plus proche, qui vous fournira les informations de retour du matériel. Envoyez ensuite l'appareil défectueux au centre de service, accompagné d'une description du problème.

LA PRESENTE GARANTIE EST LE SEUL ET EXCLUSIF RECOURS ET TIENT LIEU DE TOUTES AUTRES GARANTIES, EXPLICITES OU IMPLICITES, Y COMPRIS TOUTE GARANTIE IMPLICITE QUANT A L'APTITUDE DU PRODUIT A ETRE COMMERCIALISE OU APPLIQUE A UNE FIN OU A UN USAGE DETERMINE. FLUKE NETWORKS NE POURRA ETRE TENU RESPONSABLE D'AUCUN DOMMAGE PARTICULIER, INDIRECT, ACCIDENTEL OU CONSECUTIF, NI D'AUCUN DÉGAT OU D'AUCUNE PERTE DE DONNEES, SUR UNE BASE CONTRACTUELLE, EXTRA-CONTRACTUELLE OU AUTRE.

Etant donné que certains pays ou Etats n'admettent pas les limitations d'une condition de garantie implicite, ou l'exclusion ou la limitation de dégâts accidentels ou consécutifs, il se peut que les limitations et les exclusions de cette garantie ne s'appliquent pas à chaque acheteur.

4/04

Fluke Networks
PO Box 777
Everett, WA 98206-0777
USA

Table des matières

Accès au Manuel d'utilisation 1
Avertissements 2
  Spécifications générales 5
  Maintenance, service et problème d'équipements de protection 6
Pour contacter Fluke Networks 7
Charge et durée de vie de la batterie 8
Fenêtre d'accueil 9
Configuration minimum pour des performances optimales 12
Quelles sont les informations fournies sur votre réseau sans fil ? 13
  Quel est l'état de Mon Réseau ? 13
  Composition du réseau LAN sans fil 17
  Connectivité des périphériques au réseau sans fil 19
  Causes des ralentissements de performances réseau et des pertes de connexion 21
  Sécurité du réseau 22
  Comment puis-je trouver un point d'accès ? .. 26
  Consignation de l'état du réseau et de la session de test 26
  Comment puis-je effacer tout le contenu de mon AirCheck ? 26
Recherche de canaux, réseaux, points d'accès ou clients 27

Accès au Manuel d'utilisation

Ce guide fournit des informations de base pour vous aider à utiliser le testeur Wi-Fi AirCheck™. Pour plus d'informations, reportez-vous au mode d'emploi sur le CD du produit.

Le CD contient également l'application AirCheck Manager pour vous aider à tirer le meilleur parti de votre testeur.

Avertissements

Le testeur Wi-Fi AirCheck ™ est un outil portatif dédié permettant de vérifier et de dépanner rapidement les réseaux Wi-Fi.

⚠Avertissement⚠

Veuillez lire toutes les Consignes de sécurité avant d'utiliser le Produit.

Utilisez le produit uniquement comme spécifié, faute de quoi la protection fournie par le produit peut être compromise.

Lisez attentivement toutes les instructions.

N'utilisez que des adaptateurs secteur agrées par Fluke pour recharger la batterie.

N'utilisez pas cet appareil à proximité de gaz explosifs, de vapeurs ou dans des environnements humides ou mouillés.

Examinez le boîtier avant d'utiliser le Produit. Vérifiez qu'il ne présente ni fissures ni parties plastiques manquantes. Examinez attentivement l'isolant autour des bornes.

La batterie contient des produits chimiques dangereux qui peuvent provoquer des brûlures ou exploser. Si l'exposition aux produits chimiques survient, nettoyez avec de l'eau et demandez de l'aide médicale.

Retirez la batterie si le Produit n'est pas utilisé pendant une longue période de temps, ou s'il est stocké à des températures supérieures à 50 °C. Si la batterie n'est pas retirée, un risque de fuite de la batterie peut endommager le produit.

Ne pas court-circuiter les bornes de la batterie.

Ne pas démonter la batterie ni écraser les éléments et blocs de batteries.

Ne pas exposer les éléments et blocs de batteries à une chaleur excessive ou un incendie. Ne pas exposer à la lumière directe du soleil.

Ne pas charger les batteries en continu lorsque vous ne les utilisez pas.

Ne pas exposer la batterie à des chocs mécaniques.

Ne pas ouvrir la batterie. Elle ne contient aucune pièce réparable par l'utilisateur.

Reportez-vous au manuel du produit pour obtenir des instructions appropriées sur le chargement de la batterie

Pour éviter tout risque d'incendie, d'électrocution, de blessure et d'endommagement de l'équipement ou tout résultat de test erroné, consultez les informations de sécurité du *Manuel d'utilisation AirCheck* avant d'utiliser le testeur.

	Avertissement ou Attention : risque de détérioration ou de destruction du matériel ou du logiciel. Voir les explications dans le manuel.
	Avertissement : risque de choc électrique.
	Ne jetez pas de produits contenant des cartes de circuit dans les bennes à ordures. Consultez la législation locale pour connaître les procédures de mise au rebut.
	Cet équipement contient une radio de classe 2.
	Respect des directives de l'Union européenne.

	Conforme aux réglementations FCC, parties 15.107, 15.109.
	Approuvé par l'Association canadienne de normalisation (ACNOR).
	Respect des normes australiennes.
	Conforme aux normes CEM sud-coréennes.

Informations complémentaires sur les normes CEM sud-coréennes :

A급 기기 **(** 업무용 방송통신기자재 **)**	이 기기는 업무용 **(A** 급 **)** 전자파 적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며 **,** 가정 외의 지역에서 사용하는 것을 목적으로 합니다 **.**
Equipement de classe A (Equipement industriel de diffusion et de communications)	Cet équipement est un équipement industriel émettant des ondes électromagnétiques (classe A) et le vendeur ou l'utilisateur doit en être informé. Cet équipement peut être utilisé en tout lieu sauf à la maison.

Spécifications générales

Type de batterie : Bloc-batterie au lithium-ion amovible, rechargeable (18,5 watts/h)

Température et humidité relative de fonctionnement : (0 °C à +45 °C)

Humidité relative de fonctionnement : (% HR sans condensation) 90 % (10 °C à 35 °C)75 % (35 °C à 45 °C)

Stockage : -20 °C à +60 °C

Chocs et vibrations : aléatoires, 2 g, 5 Hz à 500 Hz (classe 2) test de chute à 1 mètre

Altitude : 4 000 m ; Stockage : 12 000 m

Sécurité : IEC/EN 61010-1

Maintenance, service et problème d'équipements de protection

· La batterie est le seul composant pouvant être remplacé par l'utilisateur. N'ouvrez jamais le boîtier, sauf pour remplacer la batterie.

· Utilisez uniquement des pièces de rechange approuvées par Fluke Networks.

· Utilisez cet appareil conformément aux instructions du fabricant afin de ne pas entraver sa protection intégrée.

· Nettoyez le boîtier à l'aide d'un chiffon doux et humide imbibé d'eau claire ou légèrement savonneuse.

Pour contacter Fluke Networks

www.flukenetworks.com

support@flukenetworks.com

+1-425-446-4519

- Australie : 61 (2) 8850-3333 ou 61 (3) 9329-0244
- Pékin : 86 (10) 6512-3435
- Brésil : 11 3759 7600
- Canada : 1-800-363-5853
- Europe : +31-(0) 40 2675 600
- Hong Kong : 852 2721-3228
- Japon : 03-6714-3117
- Corée : 82 2 539-6311
- Singapour : +65-6799-5566
- Taïwan : (886) 2-227-83199
- Etats-Unis : 1-800-283-5853

Consultez notre site Web pour la liste complète des numéros de téléphone.

Charge et durée de vie de la batterie

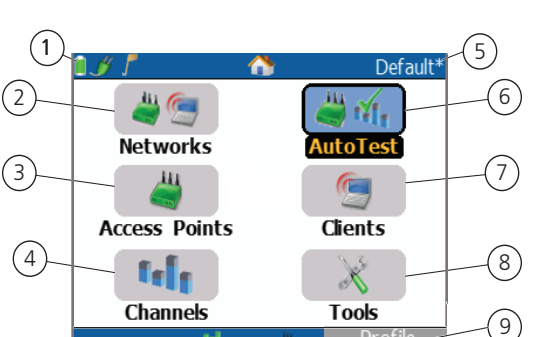
Chargez la batterie pendant 4 heures avant de l’utiliser pour la première fois. Pour charger la batterie, connectez l’adaptateur secteur au connecteur de batterie sur le testeur AirCheck.

La durée de vie de la batterie est d’environ 5,5 h en fonctionnement normal.

Indique l’état de la batterie. L’icône clignote lorsque la charge de la batterie est faible.

Indique que l’adaptateur secteur est connecté.

Fenêtre d’accueil



Accueil.eps

Figure 1. Eléments de l’écran d’accueil

① Indique l’état de la batterie. L’icône clignote lorsque la charge de la batterie est faible. Connectez l’adaptateur secteur pour charger la batterie et vous assurer que le testeur continue de fonctionner.

 Indique que l’adaptateur secteur est connecté.

 Indique que l’antenne externe est branchée.

Remarque

AirCheck ne réalise pas la transmission ou ne se connecte pas à un point d'accès lorsque l'antenne externe est connectée.

② **Réseaux** : recherche les réseaux LAN sans fil.

③ **Points d'accès** : recherche les points d'accès.

④ **Canaux** : affiche le taux d'utilisation des canaux WLAN.

⑤ Le nom du profil actuellement utilisé par le testeur. Le profil est **Par défaut** si vous n'avez pas chargé de profil différent. Le nom est suivi d'un astérisque si vous avez modifié un paramètre sur le testeur depuis le chargement ou l'enregistrement du profil.

⑥ **AutoTest** : vérifie automatiquement l'état de votre réseau en regardant la qualité de l'air (utilisation des canaux et des interférences), la qualité du réseau (couverture réseau et connectivité) et la présence de réseaux ad hoc. La détection des points d'accès indésirables est facultative et nécessite la configuration de la liste de contrôle d'autorisation (ACL).

⑦ **Clients** : recherche les clients à l'aide de vos réseaux.

⑧ **Outils** : vous permet de gérer les fichiers et les paramètres.

⑨ **Profil** : affiche une liste des profils disponibles.

⑩ Gauche : canal actuellement surveillé par le testeur. La couleur des barres indique l'état du code de pays pour le domaine réglementaire. Une icône rouge peut indiquer le fonctionnement d'un canal illégal pour le paramètre de pays actuel et/ou la réception d'un autre code de pays.

Droite : nombre de points d'accès physiques détectés par le testeur.

Jusqu'à 500 points d'accès peuvent être stockés dans la base de données du point d'accès sur le testeur. Lorsque l'icône de point d'accès devient jaune, elle indique que 400 points d'accès ou plus ont été découverts.

Lorsque cette icône devient rouge, cela indique que 500 points d'accès ou plus ont été découverts et que la base de données du point d'accès est complète. Les nouveaux points d'accès découverts ne seront pas inclus dans la liste.

Configuration minimum pour des performances optimales

Pour changer les paramètres linguistiques et nationaux

1 Sélectionnez **Outils**.

2 Pour changer la langue des écrans, sélectionnez **Définir la langue**. Mettez en surbrillance une langue, puis appuyez sur F2 **Enregistrer**.

3 Pour modifier le pays, sélectionnez **Définir le pays**, sélectionnez le pays où le testeur est utilisé, puis appuyez sur F2 **Enregistrer**.

Pour obtenir les meilleures performances de votre testeur, utilisez le logiciel AirCheck™ Manager pour configurer un profil et le charger dans le testeur. Un profil peut également être configuré sur le testeur AirCheck et contient les données qui permettent au testeur d'exécuter les tâches suivantes :

- Connexion aux réseaux exigeant des identifiants de sécurité.
- Affichage de l'état d'autorisation correct pour chaque point d'accès. Vous pouvez ainsi visualiser rapidement les points d'accès autorisés sur le réseau.
- Envoi de commandes Ping aux principaux périphériques réseau.
- Exécution d'un test de connectivité au port TCP, en utilisant un nom d'hôte ou une adresse IP et un numéro de port désigné.

Quelles sont les informations fournies sur votre réseau sans fil ?

Quel est l'état de Mon Réseau ?

- **Comment est la qualité de l'air de mon Wi-Fi ?**
  Mes canaux sont-ils surchargés par des points d'accès et un trafic Wi-Fi ?
  Mes canaux sont-ils trop bruyants ?

  Sélectionnez **AutoTest**. Après l'exécution de l'AutoTest, sélectionnez **Qualité de l'air** pour visualiser les résultats de l'utilisation 802.11 du canal, de l'utilisation autre que 802.11 du canal et de l'évaluation de l'état des interférences entre canaux.

  Les résultats de l'utilisation 802.11 du canal incluent les trois canaux les plus sollicités à avoir le trafic Wi-Fi le plus important. La valeur d'utilisation du canal et la notation ✓ Succès, ⚠ Avertissement ou ✗ Échec, sont affichées. Le résultat du test se base sur une comparaison de la valeur réelle aux seuils définissables par l'utilisateur. Ces seuils sont configurés dans **Outils > Seuils / Paramètres de l'AutoTest**.

  Les résultats de l'utilisation autre que 802.11 du canal incluent les trois canaux avec le plus d'interférences et de bruits autres que 802.11. La valeur d'utilisation du canal et la notation ✓ Succès, ⚠ Avertissement ou ✗ Echec, s'affichent.

Les résultats des interférences entre canaux incluent les trois canaux avec le plus de points d'accès ayant une puissance de signal et une qualité de signal minimales. Le nombre de points d'accès et la notation égale ou supérieure à ✓Succès, ⚠ Avertissement ou ✗ Echec, s'affichent.

- **Comment est la qualité de Mon Réseau Wi-Fi ?**
  Puis-je détecter des points d'accès prenant en charge mes réseaux ?
  Existe-t-il des trous de couverture dans cette zone ?
  Y a-t-il trop de points d'accès proches utilisant le même canal ce qui ralentit mon réseau ?
  Puis-je me connecter ?

  Sélectionnez **AutoTest** - Après l'exécution de l'AutoTest, sélectionnez **Qualité réseau** pour afficher les résultats de l'évaluation de la couverture, des interférences entre canaux, de la sécurité et de la connexion.

Les résultats de la couverture incluent l'affichage du nombre de points d'accès avec une qualité de signal bonne ainsi qu'une bonne puissance de signal et un bon rapport signal/bruit prenant en charge un réseau (SSID) et de la notation ✓Succès, ⚠ Avertissement ou ✗ Echec. La note du test se base sur une comparaison des valeurs réelles par rapport aux seuils définissables par l'utilisateur. Le nombre de points d'accès et les seuils de qualité de signal du niveau de signal et du rapport signal/bruit sont définis dans les écrans **Outils > Seuils / Paramètres de l'AutoTest > Couverture des points d'accès, Niveau de signal** et **Seuil rapport signal/bruit**.

Les résultats des interférences entre canaux incluent le nombre de points d'accès se chevauchant pour un réseau et la notation ✓Succès, ⚠ Avertissement ou ✗ Echec, basés sur une simple comparaison du réseau aux seuils. Les seuils pour ce test sont définis dans l'écran des seuils entre canaux **Outils > Seuils / Paramètres de l'AutoTest > Qualité réseau**.

Les résultats sur la sécurité indiquent si tous les points d'accès sur le SSID utilisent les mêmes identifiants de sécurité avec la notation ✓Succès, ⚠ Avertissement ou ✗ Echec.

Le test de connexion tente de se connecter à chaque réseau configuré dans votre profil. Les résultats du test de connexion indiquent si vous pouvez vous connecter à des réseaux à votre emplacement ou non avec la notation de test Succès ou Echec. Des détails supplémentaires sur la connexion par ex., le canal, l'adresse IP reçue ou le taux de connexion sont indiqués sous la forme d'une notation ✓ Succès, ⚠ Avertissement ou ✗ Echec.

- **Quels points d'accès non autorisés ou inconnus sont connectés à mon réseau Wi-Fi ?**
  Existe-t-il un risque pour la sécurité ?

  Le test des points d'accès indésirables est une partie facultative de l'AutoTest, il indique si les points d'accès non autorisés ou inconnus sont détectés avec la notation ✓ Succès, ⚠ Avertissement ou ✗ Echec. Les résultats comprennent une liste de tous les points d'accès indésirables détectés à votre emplacement. L'identification des points d'accès indésirables requiert la configuration d'une liste de contrôle d'accès (ACL). La configuration de la liste de contrôle d'accès (ACL) est disponible depuis l'écran AutoTest en sélectionnant **Points d'accès indésirables > Liste de contrôle d'accès (ACL)** ou **Accueil> Points d'accès > Liste de contrôle d'accès (ACL)**.

Composition du réseau LAN sans fil

- **Quels sont les réseaux LAN sans fil disponibles ?**

  Sélectionnez **Réseaux** pour afficher la liste des réseaux locaux sans fil et les points d'accès qui se connectent à chaque réseau. Pour voir tous les points d'accès qui sont disponibles à votre emplacement, sélectionnez **Points d'accès**.

- **Quels sont les points d'accès disponibles ? Les signaux sont-ils suffisamment puissants ?**

  Sélectionnez **Points d'accès** pour voir la liste des points d'accès disponibles à votre emplacement et la puissance du signal des points d'accès. Pour voir les graphiques à barres du bruit et de la puissance du signal d'un point d'accès, mettez en surbrillance le point d'accès, puis appuyez sur SELECT.

- **Le point d'accès est-il correctement configuré ?**

  Sur l'écran d'accueil, sélectionnez **Points d'accès**, mettez en surbrillance un point d'accès, puis appuyez sur SELECT.

- **Y a-t-il de nouveaux points d'accès dans la zone ? S'agit-il de vos points d'accès, de points d'accès voisins ou indésirables ?**

Utilisez la fonction d'état d'autorisation du périphérique (ACL) pour signaler automatiquement la découverte de nouveaux points d'accès à votre emplacement. Pour utiliser cette fonction, configurez l'état d'autorisation du point d'accès pour chaque point d'accès (par ex., autorisé ou voisin), après avoir configuré l'état d'autorisation par défaut sur ? **Inconnu**. Par conséquent, l'état d'autorisation par défaut de ? **Inconnu** sera affecté aux points d'accès qui n'ont pas déjà été découverts. Enfin, sélectionnez **Points d'accès** sur l'écran d'accueil pour voir les points d'accès marqués comme ? **Inconnu**.

Vous pouvez également sauvegarder la session de test qui comprend la liste des points d'accès découverts. Utilisez AirCheck Manager pour comparer la liste des points d'accès à un fichier de session précédemment enregistré afin de voir si d'autres points d'accès ont été découverts.

Pour indiquer si une autorisation de périphérique par défaut est inconnue ou autorisée, sélectionnez **Outils > Définir l'autorisation du périphérique (ACL) par défaut**

- ❑ **Quels clients sans fil utilisent le réseau ?**

  Sur l'écran d'accueil, sélectionnez **Clients**. Vous pouvez également parcourir les détails des points d'accès ou des canaux pour voir la liste des clients qui leur sont associés.

Connectivité des périphériques au réseau sans fil

Le testeur permet de vérifier la connectivité.

- ❑ **Les périphériques peuvent-il se connecter à ce réseau (SSID) en tant que clients ?**

  Sélectionnez **Réseaux**, sélectionnez un réseau, puis appuyez sur F1 **Connexion**.

  Remarque

  Vous ne pouvez vous connecter aux réseaux sécurisés que si un profil avec identifiants de sécurité est configuré sur le testeur.

- ❑ **Les périphériques peuvent-il se connecter à ce point d'accès (BSSID) ?**

  Sélectionnez **Points d'accès**, mettez en surbrillance un point d'accès, puis appuyez sur F1 **Connecter**. Si un ***** se trouve à droite de **Connecter**, cela indique que la sécurité n'a pas été configurée sur le testeur pour ce réseau. Appuyez sur **Connecter*** pour être guidé à travers les paramètres de sécurité. Lorsque vous avez terminé, il est enregistré dans le profil en cours. Appuyez sur **Outils**, puis sur **Gérer les profils / Mots de passe réseau** pour éditer de nouveau les paramètres de sécurité si nécessaire.

- ❑ **En cas d'échec de la connexion d'un périphérique à un réseau ou à un point d'accès, à quel stade la connexion échoue-t-elle ?**

Consultez le journal des connexions. Appuyez sur F2 **Journal** dans l'écran **Connexion au réseau** ou dans l'écran **Connexion au point d'accès**.

- ❑ **Les périphériques peuvent-ils adresser des commandes Ping à ce périphérique réseau ?**

  Effectuez un test Ping. Connectez-vous à un réseau ou à un point d'accès, puis appuyez sur F1 **Dém. tests**.

  Remarque

  *Les cibles Ping peuvent être ajoutées en sélectionnant **Outils > Gérer les profils / mots de passe réseau > Modifier les cibles > Ajouter**. Vous pouvez ajouter une cible avec une adresse IP ou un nom d'hôte (URL).*

  *Si un ***** se trouve à droite de **Connecter**, cela indique que la sécurité n'a pas été configurée sur le testeur pour ce réseau. Appuyez sur **Connecter*** pour être guidé à travers les paramètres de sécurité.*

- ❑ **La carte réseau de ce client fonctionne-t-elle correctement ?**

  Sélectionnez **Clients**, puis recherchez dans la colonne SSID. Les SSID en pointillés sont des clients inquisiteurs et les clients dont le nom SSID est affiché sont des clients associés. Appuyez sur SELECT pour voir si le client transmet des trames de demandes de détection.

Causes des ralentissements de performances réseau et des pertes de connexion

- **L'intensité du signal est-elle suffisante ?**

  Sélectionnez **Points d'accès**. L'écran **Points d'accès** indique la puissance du signal pour chaque point d'accès. Sélectionnez un point d'accès pour obtenir plus de détails sur la puissance et l'encombrement du signal.

- **Le réseau est-il surchargé ?**

  Sélectionnez **Canaux** pour voir un aperçu de l'utilisation du canal et le nombre de points d'accès qui utilisent chaque canal. Pour afficher un graphique, mettez en surbrillance un canal, puis appuyez sur (SELECT).

- **Y a-t-il des interférences non 802.11 sur ce canal ?**

  Sélectionnez **Canaux**. Les interférences non 802.11 apparaissent en gris. Ce bruit peut interférer avec les connexions WLAN ou les performances. Le bruit non 802.11 peut provenir des fours à micro-ondes, des téléphones sans fil, des périphériques Bluetooth®, des détecteurs de mouvements, des caméras sans fil et d'autres périphériques sans fil.

  Remarque

  *Les trois mesures précédentes sont également résumées dans la fonction **AutoTest**.*

Sécurité du réseau

- **Les réseaux offrent-ils le niveau de sécurité attendu ?**

  Sélectionnez **Réseaux**. Les réseaux qui comportent des points d'accès non sécurisés sont signalés par un cadenas rouge ( ).

- **Y a-t-il des réseaux ad hoc dans la zone ?**

  Sélectionnez **Réseaux**. Les stations qui fonctionnent en mode réseau ad hoc seront marquées de l'icône ad hoc ( ) dans la colonne SSID. Les stations ad hoc peuvent représenter des risques pour la sécurité du réseau ou peuvent violer les politiques réseau.

  L'AutoTest comprend un test réseau ad hoc qui indique les stations ad hoc.

- **Y a-t-il des points d'accès indésirables dans la zone ? Quels sont-ils ?**

  AirCheck peut être utilisé pour suivre l'état d'autorisation des points d'accès découverts. Par défaut, lorsque les points d'accès sont découverts, ils sont affectés à l'état d'autorisation ? **Inconnu**. Vous pouvez modifier l'état des points d'accès individuels ou en groupes pour refléter leur relation par rapport à votre réseau p. ex., autorisé, voisin, non autorisé.

Vous avez également la possibilité de passer l'état du périphérique par défaut de ? **Inconnu** à ✓ **Autorisé**. Une fois modifié, tous les points d'accès détectés seront identifiés comme ✓ **Autorisé**. Vous pouvez alors examiner la liste et affecter l'état en fonction des points d'accès individuels. Par exemple, si vous savez qu'un point d'accès est indésirable, vous pouvez lui donner le statut périphérique **Marqué** ou périphérique ⚠ **Non autorisé**.

Pour spécifier une autorisation de périphérique par défaut, sélectionnez **Outils > Définir l'autorisation du périphérique (ACL) par défaut**.

Pour attribuer un état d'autorisation à un point d'accès ou à un groupe de points d'accès, sélectionnez **Points d'accès**, mettez en surbrillance un point d'accès, puis appuyez sur F2 **ACL**.

Vous pouvez définir l'état d'autorisation pour tous les points d'accès sur ✓**Autorisé** en sélectionnant ✓**Définir tous les points d'accès sur Autorisé**. Tous les points d'accès détectés seront alors marqués comme ✓**Autorisé**. En utilisant cette approche, lorsque l'état d'autorisation par défaut est ensuite défini sur ? **Inconnu**, les points d'accès nouvellement découverts seront indiqués comme ? **Inconnu**. Globalement, cette méthode permet une visibilité rapide des risques de sécurité ou des nouveaux points d'accès.

Vous pouvez également définir une série de points d'accès autorisés ou non autorisés en fonction du point d'accès BSSID/MAC ou du préfixe MAC de fournisseur en sélectionnant ✓**Définir la série de points d'accès sur Autorisé** ou ⚠**Définir la série de points d'accès sur Non autorisé**. Ces options peuvent vous faire gagner du temps lors de la configuration et assurer une visibilité rapide des problèmes potentiels. Par exemple, si l'équipement d'un fournisseur spécifique n'est pas autorisé par votre politique réseau, utilisez le préfixe MAC de fournisseur pour définir la liste de contrôle d'autorisation (ACL) sur non autorisé. Lorsque ces points d'accès sont détectés, ils seront automatiquement signalés comme non autorisés.

Remarque

Lorsque vous enregistrez votre profil, les listes de contrôle d'autorisation affectées seront également sauvegardées sous ce profil.

L'AutoTest inclut éventuellement un test des points d'accès indésirables qui détecte et signale les points d'accès non autorisés. Pour activer cette fonctionnalité, accédez à **Outils > Seuils/ Paramètres de l'AutoTest > AutoTest des points d'accès indésirables**. Pour obtenir des résultats de tests exacts et significatifs, vous devez configurer les listes de contrôle d'autorisation des points d'accès avant d'exécuter l'AutoTest.

Comment puis-je trouver un point d'accès ?

Sélectionnez **Points d'accès**, sélectionnez un point d'accès, puis appuyez sur F2 **Localiser** sur l'écran **Détails du point d'accès**. Vous pouvez également utiliser l'antenne directionnelle externe de Fluke Networks disponible en option pour vous aider à trouver des points d'accès plus rapidement.

Consignation de l'état du réseau et de la session de test

Appuyez sur pour sauvegarder la session, puis utilisez le logiciel AirCheck Manager pour télécharger les données sur un PC et créer un rapport.

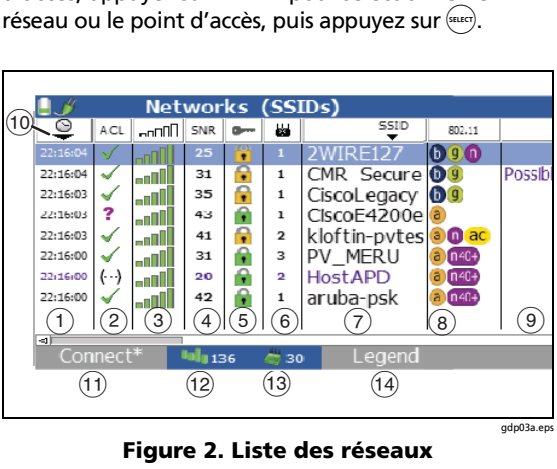
Comment puis-je effacer tout le contenu de mon AirCheck ?

Si vous souhaitez effacer tous les paramètres, toutes les données de session et tous les profils du testeur, sélectionnez **Outils > Effacer tout** - Tout ce qui a été enregistré ou stocké sur le testeur AirCheck est effacé.

Recherche de canaux, réseaux, points d'accès ou clients

Pour rechercher des canaux, des réseaux, des points d'accès ou des clients, sélectionnez **Canaux**, **Réseaux, Points d'accès,** ou **Clients** sur l'écran d'accueil. La figure 2 affiche une liste des **Réseaux**.

Pour afficher les détails d'un réseau ou d'un point d'accès, appuyez sur ▲ ▼ pour sélectionner le réseau ou le point d'accès, puis appuyez sur SELECT.



gdp03a.eps

Figure 2. Liste des réseaux

① : L'heure à laquelle le testeur a été détecté pour la première fois. Pour voir les réseaux qui deviennent disponibles à mesure que vous vous déplacez, triez la liste par ordre décroissant d'après la colonne d'horodatage.

Appuyez sur , puis parcourez une zone. Les réseaux qui deviennent disponibles sont ajoutés en haut de la liste. Les réseaux qui deviennent indisponibles deviennent gris si **Griser points d'accès inaudibles** est activé.

② **ACL :** L'état d'autorisation du point d'accès. L'état par défaut est ? **Inconnu**, mais peut être remplacé par ✓ **Autorisé**. Modifiez l'état de chaque point d'accès pour afficher la façon dont il est lié à votre réseau. Pour changer l'état, sélectionnez **Points d'accès** sur l'écran d'accueil, sélectionnez un point d'accès, puis appuyez sur F2 **ACL**.

(...) : les points d'accès sur le réseau n'ont pas tous le même état d'autorisation.

③ ▁▃▅▇ : intensité maximum du signal de tous les points d'accès pour un identifiant SSID réseau donné.

④ **SNR :** le rapport signal/bruit est une mesure de puissance du signal par rapport au bruit. Le rapport est mesuré en décibels (dB).

⑤ : état de sécurité du réseau :

Cadenas ouvert rouge : le réseau n'est pas sécurisé.

Remarque

Certains réseaux avec un cadenas ouvert vous permettent de connecter le testeur et d'effectuer des mesures y compris d'exécuter le test Ping, mais peuvent ne pas permettre à un ordinateur de se connecter au même réseau pour se connecter au Web sans ID d'utilisateur et mot de passe.

Cadenas fermé jaune : au moins un point d'accès applique les protocoles de sécurité WEP ou Cisco LEAP. Ceux-ci sont moins sécurisés que les autres protocoles.

Cadenas fermé vert : tous les points d'accès appliquent des protocoles de sécurité plus fiables que WEP, par exemple WPA ou WPA2.

(...) : Tous les points d'accès dans le réseau n'utilisent pas le même type de sécurité. Par exemple, l'un utilise le protocole WEP et l'autre utilise le protocole WPA.

⑥ : nombre de points d'accès que le testeur détecte dans la zone.

⑦ **SSID** : Identificateur SSID (Service Set Identifier). Le nom du réseau sans fil.

: Le réseau comporte des périphériques ad hoc. Il s'agit de périphériques qui communiquent directement avec les autres périphériques, non pas à travers un point d'accès. Les périphériques ad hoc peuvent permettre aux pirates informatiques d'accéder aux données transmises sur le réseau. (Certaines stratégies informatiques pour réseaux autorisent les périphériques ad hoc.)

[Caché] : le réseau ne diffuse pas son identifiant SSID.

⑧ **802.11** : normes 802.11 utilisées par les points d'accès du réseau :

802.11a : bande 5 GHz

802.11b : bande 2,4 GHz

802.11g : bande 2,4 GHz

802.11n : utilise la bande 2,4 GHz ou 5 GHz.

802.11ac : utilise la bande 5 GHz.

Barres rouges : le testeur a reçu un code de pays qui est différent du paramètre dans **Outils** > **Définir le pays**. Pour identifier le réseau ou le point d'accès qui transmet le code, sélectionnez **Réseaux** ou **Points d'accès**, puis recherchez les barres rouges dans la colonne **802.11**.

n40+ n40– : Un ou plusieurs points d'accès utilisent un canal couplé. Les points d'accès qui utilisent la norme 802.11n peuvent lier un canal avec un canal d'extension supérieur (n40+) ou inférieur (n40–) pour créer un canal de 40 MHz. Ce plus grand canal fournit au réseau un débit plus élevé.

(...) : les points d'accès du réseau n'utilisent pas tous la même norme 802.11.

⑨ **Remarques** : Appuyez sur ▷ pour faire défiler le champ des remarques. Le testeur ajoute les remarques automatiquement. Les réseaux qui comportent des remarques sont indiqués en violet.

(...) : Le réseau comporte plusieurs remarques. Pour afficher toutes les remarques, sélectionnez le réseau, puis appuyez sur SELECT deux fois pour afficher l'écran **Détails du point d'accès**.

⑩ ▼▲ : **Tri 1**, ordre de tri croissant ou décroissant.

▼ ▲ : **Tri 2**, ordre de tri croissant ou décroissant.

Pour trier la liste par ordre croissant ou décroissant, appuyez sur △ et sur ◁ ▷ pour sélectionner un en-tête de colonne, puis appuyez sur SELECT ou F1 **Tri 1**. Par exemple, pour retrouver facilement le point d'accès avec le signal le plus fort, sélectionnez ▁▃▅▇ en haut de la colonne, puis appuyez sur SELECT ou F1 **Tri 1**. Le point d'accès avec le signal le plus fort est placé en haut de la liste.

Pour appliquer un ordre de tri secondaire, sélectionnez un autre en-tête de colonne, puis appuyez sur F2 **Tri 2**.

⑪ Appuyez sur F1 **Connexion** pour vous connecter au réseau sélectionné.

Le bouton de connexion apparaît sous **Connecter*** (avec un astérisque) si le testeur ne peut pas se connecter au réseau mis en surbrillance. Pour configurer les paramètres de sécurité du réseau, appuyez sur F1 **Connecter***.

Remarque

Pour vous connecter à un réseau sécurisé, le testeur doit avoir un profil qui contient les identifiants de sécurité. Créez ou modifiez les identifiants de sécurité sur le testeur ou avec AirCheck Manager. Lorsque vous appuyez sur ***Connecter**** *sur le testeur, vous êtes guidé à travers la configuration de la sécurité. Vous pouvez également appuyer sur* ***Outils****, puis sur* ***Gérer les profils /mots de passe réseau*** *pour reconfigurer les paramètres de sécurité. Le* ***** *à droite de* ***Connecter*** *indique qu'aucun paramètre de sécurité n'a été configuré. Reportez-vous au manuel d'utilisation pour la configuration des procédures de sécurité à l'aide de Connecter.*

⑫

: canal actuellement utilisé par le testeur. La couleur des barres indique l'état du code de pays pour le domaine réglementaire.

⑬ : nombre de points d'accès détectés par le testeur à votre emplacement. Ce chiffre n'inclut pas les points d'accès virtuels si l'option **Regrouper points d'accès virtuels** est sélectionnée.

⑭ Pour afficher la description des icônes de l'écran **Réseaux**, appuyez sur F2 **Légende**.

Pour afficher les détails des points d'accès d'un réseau, appuyez sur ▲ ▼ pour sélectionner un réseau, puis appuyez sur SELECT.

FLUKE networks

AirCheck™
Wi-Fi-Tester

Erste Schritte

PN 3434814 12/2009 Rev. 4, 8/13 (German)
©2009-2013 Fluke Corporation. Printed in USA.
All product names are trademarks of their respective companies.
Wi-Fi® is a registered trademark of the Wi-Fi Alliance.

BESCHRÄNKTE GEWÄHRLEISTUNG UND HAFTUNGSBEGRENZUNG

Fluke Networks gewährleistet, dass dieses Produkt für den Zeitraum von einem Jahr ab Kaufdatum frei von Material- und Fertigungsdefekten ist Die Gewährleistungsdauer für Einzelteile, Zubehör, Produktreparaturen und Serviceleistungen beträgt 90 Tage, sofern nicht anders vermerkt. NiCd-, NiMH- und Li-Ionen-Akkus, Kabel oder andere Peripheriegeräte gelten als Einzelteile bzw. Zubehör.

Diese Gewährleistung gilt nicht für Schäden durch Unfälle, Vernachlässigung, Missbrauch, Modifikation, Verunreinigung bzw. irreguläre Betriebsbedingungen oder unsachgemäße Handhabung. Diese Gewährleistung darf von keiner Verkaufsstelle im Namen von Fluke Networks verlängert werden.

Um während des Gewährleistungszeitraums Leistungen in Anspruch zu nehmen, wenden Sie sich an das nächstgelegene autorisierte Servicecenter von Fluke Networks, um Informationen zur Rücksendeautorisierung zu erhalten. Senden Sie das beschädigte Produkt mit einer Beschreibung des Problems an das zuständige Servicecenter.

DIESE GEWÄHRLEISTUNG IST IHR EINZIGER RECHTSANSPRUCH. ES BESTEHEN KEINE WEITEREN AUSDRÜCKLICH ODER STILLSCHWEIGEND EINGESCHLOSSENEN GARANTIEN, WIE Z. B. DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. FLUKE NETWORKS HAFTET NICHT FÜR SPEZIELLE, UNMITTELBARE, NEBEN- ODER FOLGESCHÄDEN ODER VERLUSTE, UNABHÄNGIG VON DER URSACHE ODER THEORIE.

Weil einige Staaten oder Länder den Ausschluss oder die Einschränkung einer implizierten Gewährleistung sowie von Begleit- oder Folgeschäden nicht zulassen, ist diese Gewährleistungsbeschränkung möglicherweise für Sie nicht gültig.

4/04

Fluke Networks
PO Box 777
Everett, WA 98206-0777
USA

Inhalt

Zugriff auf das Benutzerhandbuch..... 1
Warninformationen..... 2
Allgemeine Spezifikationen..... 5
Wartung, Service und Beeinträchtigung der Gerätesicherheit..... 6
Kontaktaufnahme mit Fluke Networks 7
Laden und Betriebsdauer des Akkus 8
Startbildschirm 9
Mindestkonfiguration für bestmögliche Leistung..... 12
Welche Informationen erhalten Sie über Ihr WLAN? 13
In welchem Zustand befindet sich mein Netzwerk?..... 13
Was befindet sich im WLAN?..... 18
Können Geräte eine Verbindung zum WLAN herstellen?..... 20
Was ist der Grund für schwache Netzwerkleistung oder Verbindungsverluste?..... 22
Weist das Netzwerk Sicherheitsrisiken auf?.... 23
Wie kann ich einen Access Point orten?..... 27
Wie kann ich mein Netzwerk und meine Testsitzung dokumentieren? 27
Wie kann ich alle Daten von meinem AirCheck löschen?..... 27
Finden von Kanälen, Netzwerken, APs oder Clients 28

Zugriff auf das Benutzerhandbuch

Diese Anleitung bietet allgemeine Informationen und erste Schritte zur Verwendung des AirCheck™ Wi-Fi-Testers. Weitere Informationen finden Sie im Benutzerhandbuch auf der Produkt-CD.

Ebenfalls auf der CD enthalten ist die Applikation „AirCheck Manager“, mit deren Hilfe Sie Ihren Tester optimal nutzen können.

Warninformationen

Der AirCheck ™ Wi-Fi-Tester ist ein spezielles Handheld-Tool zur schnellen Überprüfung und Fehlerbehebung in WLAN-Netzwerken.

⚠ Warnung ⚠

Lesen Sie alle Sicherheitshinweise, bevor Sie das Gerät verwenden.

Verwenden Sie das Gerät nur wie angegeben, oder der vom Gerät bereitgestellte Schutz kann beeinträchtigt werden.

Lesen Sie alle Anweisungen sorgfältig durch.

Verwenden Sie nur von Fluke zugelassene Netzteile, um den Akku aufzuladen.

Setzen Sie das Gerät nicht in der Nähe von explosiven Gasen, Dämpfen oder in feuchten oder nassen Umgebungen ein.

Prüfen Sie das Gehäuse, bevor Sie das Gerät verwenden. Achten Sie auf Risse oder fehlenden Kunststoff. Sehen Sie sich die Isolierung um die Anschlüsse sorgfältig an.

Akkus enthalten gefährliche Chemikalien, die Verbrennungen hervorrufen oder zu einer Explosion führen können. Reinigen Sie sich bei Kontakt mit Chemikalien mit Wasser, und fordern Sie medizinische Hilfe an.

Entfernen Sie die Akkus, wenn das Gerät für längere Zeit nicht verwendet wird oder wenn es bei Temperaturen über 50 °C gelagert wird. Wenn die Akkus nicht entfernt werden, können sie auslaufen und das Gerät beschädigen.

Schließen Sie den Akku nicht mit den Anschlüssen kurz.

Nehmen Sie die Akkuzellen oder Akkusätze nicht auseinander, und zerdrücken Sie sie nicht.

Setzen Sie keine Akkuzellen und Akkusätze in der Nähe von Hitze oder Feuer ein. Schützen Sie sie vor Sonnenlicht.

Laden Sie Akkus nicht ständig auf, wenn sie nicht verwendet werden.

Setzen Sie die Akkusätze keinen mechanischen Erschütterungen aus.

Öffnen Sie den Akkusatz nicht. Dieser enthält keine vom Benutzer zu wartenden Teile.

Lesen Sie die Bedienungsanleitung mit den Anweisungen zum ordnungsgemäßen Aufladen des Akkusatzes durch.

Um Feuer, Stromschlag, Verletzungen, Beschädigung von Ausrüstung oder ungenaue Testergebnisse zu vermeiden, lesen Sie vor Gebrauch des Testers die Sicherheitsinformationen im *AirCheck Bedienungshandbuch.*

	Warnung oder Vorsicht: Risiko der Beschädigung oder Zerstörung von Gerät oder Software. Siehe Erläuterungen im Benutzerhandbuch.
	Warnung: Risiko von Stromschlägen.
	Produkte, die über Leiterplatten verfügen, dürfen nicht in Abfallbehältern entsorgt werden. Die Entsorgungsregelungen für Ihre Region entnehmen Sie bitte den örtlichen Bestimmungen und Vorschriften.
	Dieses Gerät enthält ein Klasse-2-Funkgerät.
	Erfüllt die entsprechenden EU-Richtlinien.

	Entspricht den FCC-Vorgaben, Teile 15.107, 15.109.
	Aufgeführt durch die Canadian Standards Association.
	Erfüllt die entsprechenden australischen Standards.
	Erfüllt die entsprechenden südkoreanischen EMV-Standards.

Zusatzinformationen zu südkoreanischen EMV-Standards:

A급 기기 **(업무용** **방송통신기자재)**	**이 기기는 업무용 (A 급) 전자파 적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며 , 가정 외의 지역에서 사용하는 것을 목적으로 합니다 .**
Gerät der Klasse A (Geräte für die industrielle Rundfunkübertragung und -kommunikation)	Dieses Produkt erfüllt die Anforderungen für industrielle Geräte mit elektromagnetischer Strahlung (Klasse A), und der Verkäufer oder Benutzer sollte darüber informiert sein. Dieses Gerät ist für die Verwendung in verschiedenen Anwedungsbereichen, jedoch nicht für die Heimanwendung, geeignet.

Allgemeine Spezifikationen

Akku-Typ: Auswechselbarer, wiederaufladbarer Lithium-Ionen-Akkusatz (18,5 Wattstunden)

Betriebstemperatur und relative Luftfeuchtigkeit: (0 °C bis 45 °C)

Relative Luftfeuchtigkeit bei Betrieb (% RL, nicht kondensierend)90 % (10 °C bis 35 °C), 75 % (35 °C bis 45 °C)

Lagerung: - 20 °C bis + 60 °C

Stoß- und Vibrationsfestigkeit: Zufällig, 2 g, 5 Hz – 500 Hz (Klasse 2), Fallprüfung aus 1 m Höhe

Höhe: 4.000 m, Lagerung: 12.000 m

Sicherheit: IEC/EN 61010-1

Wartung, Service und Beeinträchtigung der Gerätesicherheit

· Der Akku ist die einzige vom Benutzer zu wartende Komponente. Öffnen Sie das Gehäuse nicht, es sei denn, Sie möchten den Akku ersetzen.

· Verwenden Sie nur Ersatzteile, die von Fluke Networks genehmigt sind.

· Wird dieses Gerät nicht entsprechend den Herstellerangaben bestimmungsgemäß eingesetzt, können die Sicherheitseinrichtungen des Geräts eventuell beeinträchtigt werden.

· Verwenden Sie zum Reinigen des Gehäuses ein weiches, leicht mit Wasser oder mit Wasser und einem milden Reinigungsmittel angefeuchtetes Tuch.

Kontaktaufnahme mit Fluke Networks

www.flukenetworks.com

support@flukenetworks.com

+1-425-446-4519

- Australien: 61 (2) 8850-3333 oder 61 (3) 9329-0244
- Peking: 86 (10) 6512-3435
- Brasilien: 11 3759 7600
- Kanada: 1-800-363-5853
- Europa: +31 (0) 40 2675 600
- Hongkong: 852 2721-3228
- Japan: 03-6714-3117
- Korea: 82 2 539-6311
- Singapur: +65-6799-5566
- Taiwan: (886) 2-227-83199
- USA: 1-800-283-5853

Die vollständige Liste der Telefonnummern steht auf der Website zur Verfügung.

Laden und Betriebsdauer des Akkus

Laden Sie den Akku vor dem ersten Einsatz 4 Stunden lang auf. Schließen Sie das Netzteil zum Aufladen des Akkus an den Steckverbinder des Akkus für den AirCheck-Tester an.

Die Akku-Betriebsdauer beträgt bei normalem Betrieb etwa 5,5 Stunden.

Zeigt den Ladestand des Akkus an. Bei schwacher Akkuladung blinkt das Symbol.

Zeigt an, dass das Netzteil angeschlossen ist.

Startbildschirm

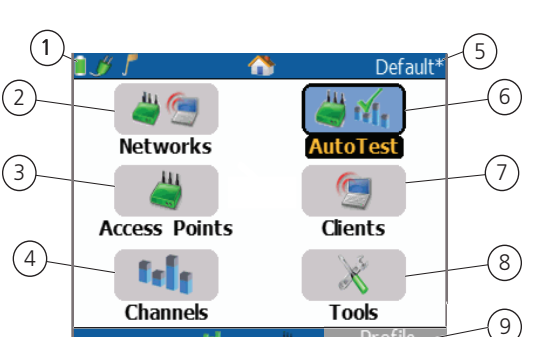


Abbildung 1. Startbildschirm-Komponenten

①

Zeigt den Ladestand des Akkus an. Bei schwacher Akkuladung blinkt das Symbol. Schließen Sie das Netzteil an den Akku an, um ihn aufzuladen und um sicherzustellen, dass der Tester weiterhin im Betrieb ist.

Zeigt an, dass das Netzteil angeschlossen ist.

Zeigt an, dass die externe Antenne angeschlossen ist.

Hinweis

Wenn die externe Antenne angeschlossen ist, sendet der AirCheck keine Daten und baut keine Verbindung mit einem Access Point auf.

② **Netzwerke**: ermittelt WLANs.

③ **Access Points**: ermittelt Access Points.

④ **Kanäle**: zeigt die Auslastung von WLAN-Kanälen an.

⑤ Der Name des derzeit vom Tester verwendeten Profils. Das Profil ist auf **Standard** eingestellt, wenn Sie kein anderes Profil geladen haben. Der Name erscheint mit einem Sternchen, wenn seit dem Laden/Speichern des Profils eine Einstellung auf dem Tester verändert wurde.

⑥ **AutoTest:** überprüft automatisch den Zustand Ihres Netzwerks durch eine Analyse der Verbindungsqualität (Kanalauslastung und Störungen), Netzwerkqualität (Netzwerkabdeckung und Verbindungsaufbau) und der Präsenz von Ad-hoc-Netzwerken. Die Erkennung nicht autorisierter Access Points ist optional und erfordert die Konfiguration einer Authorization Control List (ACL).

⑦ **Clients:** ermittelt Clients, die Ihre Netzwerke verwenden.

⑧ **Tools**: ermöglicht die Verwaltung von Dateien und Einstellungen.

⑨ **Profil:** zeigt eine Liste aller verfügbaren Profile an.

⑩ Links: der Kanal, der derzeit vom Tester überwacht wird. Die Farbe der Balken zeigt den Status des Ländercodes für die vorgeschriebene Domäne an. Ein rotes Symbol kann anzeigen, dass sich ein Kanal im Betrieb befindet, der für die aktuelle Ländereinstellung und/oder den Empfang eines anderen Ländercodes illegal ist.

Rechts: die Anzahl der vom Tester wahrgenommenen physischen Access Points.

In der Access-Point-Datenbank des Testers können bis zu 500 Access Points gespeichert werden. Verändert sich die Farbe des Access-Point-Symbols zu Gelb, so bedeutet das, dass eine Anzahl von 400 oder mehr Access Points ermittelt wurde.

Verändert sich die Farbe des Symbols zu Rot, so bedeutet das, dass eine Anzahl von 500 oder mehr Access Points ermittelt wurde und die Access-Point-Datenbank voll ist. Alle neu ermittelten Access Points werden nicht mehr in die Liste aufgenommen.

Mindestkonfiguration für bestmögliche Leistung

Ändern der Sprach- und Ländereinstellungen

1 Wählen Sie **Tools** aus.

2 Um die Sprache für die Bildschirme zu ändern, wählen Sie **Sprache einstellen** aus. Markieren Sie eine Sprache und drücken Sie dann F2 **Speichern**.

3 Um die Ländereinstellung zu ändern, wählen Sie **Land einstellen** aus, wählen Sie dann das Land aus, in dem der Tester verwendet wird, und drücken Sie dann F2 **Speichern**.

Um die bestmögliche Leistung von Ihrem Tester zu erhalten, verwenden Sie die AirCheck™ Manager-Software, um ein Profil zu konfigurieren und dieses auf den Tester hochzuladen. Ein Profil kann auch auf dem AirCheck-Tester konfiguriert werden und enthält Daten, durch die der Tester die folgenden Aufgaben ausführen kann:

- Herstellen einer Verbindung zu Netzwerken, die Sicherheitsdaten erfordern.
- Anzeigen des korrekten Autorisierungsstatus für jeden Access Point. So können Sie rasch erkennen, welche Access Points autorisierte Bestandteile des Netzwerks sind.
- Pingen von wichtigen Netzwerkgeräten.
- Durchführen eines TCP-Port-Verbindungstests unter Verwendung eines Hostnamens oder einer IP-Adresse und einer festgelegten Portnummer.

Welche Informationen erhalten Sie über Ihr WLAN?

In welchem Zustand befindet sich mein Netzwerk?

- **Wie ist die Qualität meiner Wi-Fi-Umgebung?**
  Sind meine Kanäle durch Access Points und Wi-Fi-Datenverkehr überlastet?
  Gibt es auf irgendwelchen meiner Kanäle zu viele Störungen?

  Wählen Sie **AutoTest** aus. Sobald das Ausführen des AutoTests abgeschlossen ist, wählen Sie **Verbindungsqualität** aus, um die Ergebnisse für „802.11-Kanalauslastung“, „Nicht-802.11-Kanalauslastung“ und „Zustandsbewertung der Nebenkanalstörungen“ anzuzeigen.

  Die Ergebnisse für „802.11-Kanalauslastung“ beinhalten die drei aktivsten Kanäle mit dem meisten Wi-Fi-Datenverkehr. Der Wert für die Auslastung des Kanals wird zusammen mit einer Bewertung von entweder ✓ Bestanden, ⚠ Warnung, oder ✗ Nicht bestanden angezeigt. Die Testbewertung basiert auf einem Vergleich des tatsächlichen Werts mit vom Benutzer einstellbaren Schwellenwerten. Diese Schwellenwerte sind konfigurierbar unter **Tools > Schwellenwerte/AutoTest-Einstellungen**.

Die Ergebnisse für „Nicht-802.11-Kanalauslastung“ beinhalten die drei Kanäle mit den meisten Nicht-802.11-Störungen. Der Wert für die Auslastung des Kanals wird zusammen mit einer Bewertung von entweder ✓Bestanden, ⚠ Warnung, oder ✗ Nicht bestanden angezeigt.

Die Ergebnisse für „Nebenkanalstörungen“ beinhalten die Kanäle mit den meisten APs mit einer minimalen Signalstärke und Signalqualität. Die AP-Anzahl wird zusammen mit einer Bewertung von oder höher als ✓Bestanden, ⚠ Warnung, oder ✗ Nicht bestanden angezeigt.

- **Wie hoch ist die Netzwerkqualität meines Wi-Fi-Netzwerks?**
  Kann ich Access Points wahrnehmen, die meine Netzwerke unterstützen?
  Gibt es Abdeckungslücken in diesem Gebiet?
  Gibt es in der Nähe zu viele APs, die denselben Kanal verwenden und dadurch mein Netzwerk verlangsamen?
  Kann ich eine Verbindung aufbauen?

  Wählen Sie **AutoTest** aus. Sobald das Ausführen des AutoTests abgeschlossen ist, wählen Sie **Netzwerkqualität** aus, um die Ergebnisse für Abdeckung, Nebenkanalstörungen, Sicherheit und Zustandsbewertung der Verbindung anzuzeigen.

Die Ergebnisse für „Abdeckung“ beinhalten die Anzahl der APs, die eine gute Signalqualität, d. h. sowohl eine hohe Signalstärke als auch ein gutes Signal-Rausch-Verhältnis, aufweisen und ein Netzwerk (SSID) unterstützen, und werden zusammen mit einer Bewertung von ✓ Bestanden, ⚠ Warnung, oder ✗ Nicht bestanden angezeigt. Die Testbewertung basiert auf einem Vergleich der tatsächlichen Werte mit vom Benutzer einstellbaren Schwellenwerten. Die AP-Anzahl und Schwellenwerte für die Signalqualität bestehend aus Signalstärke und Signal-Rausch-Verhältnis sind konfigurierbar auf den Bildschirmen **Tools > Schwellenwerte/Auto-Test-Einstellungen > AP-Abdeckung, Schwellenwert für Signalstärke** und **Signal-Rausch-Verhältnis**.

Die Ergebnisse für „Nebenkanalstörungen“ beinhalten die Anzahl an überlappenden APs für ein Netzwerk zusammen mit einer Bewertung von ✓ Bestanden, ⚠ Warnung, oder ✗ Nicht bestanden, basierend auf dem Vergleich eines einzelnen Netzwerks mit Schwellenwerten. Schwellenwerte für diesen Test sind konfigurierbar auf dem Bildschirm unter **Tools > Schwellenwerte/AutoTest-Einstellungen > Schwellenwerte für Netzwerkqualität von Nebenkanälen**.

Die Ergebnisse für „Sicherheit“ zeigen an, ob alle SSID-APs dieselben Sicherheitsanmeldeinformationen verwenden, zusammen mit einer Bewertung von Bestanden, Warnung, oder Nicht bestanden.

Beim Verbindungstest wird versucht, mit jedem in Ihrem Profil konfigurierten Netzwerk eine Verbindung aufzubauen. Die Ergebnisse des Verbindungstests geben an, ob Sie mit den an Ihrem Standort verfügbaren Netzwerken eine Verbindung aufbauen können oder nicht, dargestellt durch eine Bewertung von „Bestanden“ oder „Nicht bestanden“. Zusätzliche Details zur Verbindung, wie zum Beispiel der Kanal, die empfangene IP-Adresse und die Verbindungsrate werden angezeigt mit einer Bewertung von Bestanden, Warnung, oder Nicht bestanden.

- **Welche nicht autorisierten oder unbekannten Access Points sind mit meinem Wi-Fi-Netzwerk verbunden? Stellen sie ein Sicherheitsrisiko dar?**

  Der Test „Nicht autorisierte Access Points“ ist eine optionale Komponente des AutoTests, und gibt an, ob nicht autorisierte oder unbekannte Access Points ermittelt wurden, zusammen mit einer Bewertung von ✓ Bestanden, ⚠ Warnung, oder ✗ Nicht bestanden. Die Ergebnisse beinhalten eine Liste aller nicht autorisierten Access Points, die an Ihrem Standort wahrgenommen wurden. Die Identifizierung von nicht autorisierten Access Points erfordert die Konfiguration einer Access Control List (ACL). Die ACL-Konfiguration ist auf dem AutoTest-Bildschirm verfügbar durch Auswählen von **Nicht autorisierte Access Points > ACL** oder **Startbildschirm > Access Points > ACL**.

Was befindet sich im WLAN?

- ❑ **Welche WLANs sind verfügbar?**

  Wählen Sie **Netzwerke** aus, um eine Liste der WLANs und Access Points anzuzeigen, die mit den jeweiligen Netzwerken verbunden sind. Um alle an Ihrem Standort verfügbaren Access Points anzuzeigen, wählen Sie **Access Points**.

- ❑ **Welche Access Points sind verfügbar? Ist die Stärke der jeweiligen Signale ausreichend?**

  Wählen Sie **Access Points** aus, um eine Liste der an Ihrem Standort verfügbaren Access Points sowie deren Signalstärke anzuzeigen. Um Balkendiagramme der Signalstärke und Störungen für einen Access Point anzuzeigen, markieren Sie den Access Point, und drücken Sie dann (SELECT).

- ❑ **Ist der Access Point richtig konfiguriert?**

  Wählen Sie auf dem Startbildschirm **Access Points** aus, markieren Sie einen Access Point, und drücken Sie dann (SELECT).

- ❑ **Gibt es neue Access Points in Ihrem Gebiet? Handelt es sich dabei um Ihre eigenen, die Ihrer Nachbarn, oder um nicht autorisierte Access Points?**

Verwenden Sie die Gerätefunktion für den Autorisierungsstatus (ACL), um automatisch anzuzeigen, wenn an Ihrem Standort neue Access Points ermittelt wurden. Um diese Funktion zu verwenden, konfigurieren Sie den Access-Point-Autorisierungsstatus für jeden Access Point (beispielsweise „autorisiert" oder „Nachbar"), und setzen Sie danach den Standard-Autorisierungsstatus auf ? **Unbekannt**. Dadurch wird jedem Access Point, der bisher noch nicht ermittelt wurde, der Standard-Autorisierungsstatus ? **Unbekannt** zugeteilt. Wählen Sie zum Schluss auf dem Startbildschirm **Access Points** aus, um alle als ? **Unbekannt** gekennzeichneten Access Points anzuzeigen.

Alternativ können Sie auch die Testsitzung, die eine Liste der ermittelten Access Points enthält, abspeichern. Verwenden Sie dann AirCheck Manager, um die Liste der Access Points mit der Datei einer zuvor gespeicherten Sitzung zu vergleichen und festzustellen, ob zusätzliche Access Points ermittelt wurden.

Um eine Standard-Autorisierung von entweder „Unbekannt" oder „Autorisiert" auf dem Gerät festzulegen, wählen Sie **Tools > Standard-Autorisierung (ACL) einstellen**

- **Von welchen WLAN-Clients wird das Netzwerk genutzt?**

  Wählen Sie auf dem Startbildschirm **Clients** aus. Sie können auch AP-Details oder Kanal-Details anzeigen, um eine Liste der verbundenen Clients zu erhalten.

Können Geräte eine Verbindung zum WLAN herstellen?

Benutzen Sie den Tester zum Prüfen der Netzwerkverbindung.

- **Kann ein Gerät als Client eine Verbindung zum Netzwerk (SSID) herstellen?**

  Wählen Sie **Netzwerke**, markieren Sie ein Netzwerk, und drücken Sie dann F1 **Verbinden**.

  Hinweis

  Um eine Verbindung mit einem sicheren Netzwerk herzustellen, benötigt der Tester ein Profil, welches Sicherheitsdaten beinhaltet.

- **Kann ein Gerät eine Verbindung zu einem Access Point (BSSID) herstellen?**

  Wählen Sie **Access Points** aus, markieren Sie einen Access Point, und drücken Sie dann F1 **Verbinden**. Falls ein ***** auf der rechten Seite von **Verbinden** angezeigt wird, so bedeutet das, dass auf dem Tester keine Sicherheitskonfiguration für dieses Netzwerk vorhanden ist. Drücken Sie **Verbinden***, und lassen Sie sich durch den Eingabevorgang für die Sicherheitseinstellungen führen. Sobald dies abgeschlossen ist, werden diese Einstellungen für das aktuelle Profil gespeichert. Drücken Sie **Tools** und dann **Profile verwalten/Netzwerk-Kennwörter**, um die Sicherheitseinstellungen bei Bedarf zu ändern.

- **Wenn ein Gerät keine Verbindung zu einem Netzwerk oder Access Point herstellen kann, woran scheitert der Verbindungsvorgang?**

  Sehen Sie sich das Verbindungsprotokoll an. Drücken Sie F2 **Protokoll**, entweder auf dem Bildschirm **Verbindung mit einem Netzwerk herstellen** oder auf dem Bildschirm **Verbindung mit einem Access Point herstellen.**

- **Kann ein Gerät ein Netzwerkgerät pingen?**

  Machen Sie einen Ping-Test. Stellen Sie eine Verbindung zu einem Netzwerk oder Access Point her, und drücken Sie dann F1 **Tests starten**.

  Hinweis

  *Ping-Ziele können durch Auswählen von **Tools > Profile verwalten/Netzwerk-Kennwörter > Ziele bearbeiten > Hinzufügen** hinzugefügt werden. Sie können ein Ziel mit einer IP-Adresse oder einen Hostnamen (URL) hinzufügen.*

  *Falls ein ***** auf der rechten Seite von **Verbinden** angezeigt wird, so bedeutet das, dass auf dem Tester keine Sicherheitskonfiguration für dieses Netzwerk vorhanden ist. Drücken Sie **Verbinden***, und lassen Sie sich durch den Eingabevorgang für die Sicherheitseinstellungen führen.*

❑ **Funktioniert die Netzwerkkarte in einem Client korrekt?**

Wählen Sie **Clients**, und sehen Sie sich dann die Spalte „SSID“ an. Gestrichelte SSIDs sind prüfende Clients und Clients mit einem angezeigten SSID-Namen sind assoziierte Clients. Drücken Sie SELECT, und stellen Sie fest, ob der Client Probe-Request-Frames überträgt.

Was ist der Grund für schwache Netzwerkleistung oder Verbindungsverluste?

❑ **Ist die Signalstärke ausreichend?**

Wählen Sie **Access Points** aus. Der Bildschirm **Access Points** gibt die Signalstärke für jeden Access Point an. Wählen Sie einen Access Point aus, um weitere Details zur Signalstärke und zu Engpässen anzuzeigen.

❑ **Ist das Netzwerk überlastet?**

Wählen Sie **Kanäle**, um eine Übersicht über die Kanalauslastung und die Anzahl der Access Points, die den jeweiligen Kanal verwenden, anzuzeigen. Um ein Diagramm anzuzeigen, markieren Sie einen Kanal, und drücken Sie dann SELECT.

- **Wird auf einem der Kanäle eine Nicht-802.11-Störung angezeigt?**

  Wählen Sie **Kanäle**. Nicht-802.11-Störungen werden grau angezeigt. Diese Störungen können WLAN-Verbindungen und deren Übertragungsleistung negativ beeinflussen. Nicht-802.11-Störungen können von Mikrowellen, schnurlosen Telefonen, Bluetooth®-Geräten, Bewegungsmeldern, WLAN-Kameras und anderen WLAN-Geräten ausgehen.

  Hinweis

  *Die letzten drei Messungen sind auch zusammengefasst in der Funktion **AutoTest** enthalten.*

Weist das Netzwerk Sicherheitsrisiken auf?

- **Verfügen die Netzwerke über die erwartete Sicherheitsstufe?**

  Wählen Sie **Netzwerke**. Netzwerke mit ungesicherten Access Points sind durch ein rotes Schloss ( ) gekennzeichnet.

- **Gibt es in der Umgebung Ad-hoc-Netzwerke?**

  Wählen Sie **Netzwerke**. Stationen, die im Ad-hoc-Netzwerkmodus arbeiten, sind durch das Ad-hoc-Symbol ( ) in der Spalte „SSID“ gekennzeichnet. Ad-hoc-Stationen können ein Risiko für die Netzwerksicherheit darstellen oder gegen Netzwerkrichtlinien verstoßen.

Der AutoTest enthält einen Ad-hoc-Netzwerktest, der Ad-hoc-Stationen kennzeichnet.

- ❑ **Gibt es nicht autorisierte Access Points in der Umgebung? Wo genau befinden diese sich?**

  AirCheck kann als Hilfsmittel verwendet werden, um den Autorisierungsstatus von ermittelten Access Points zu verfolgen. Sobald Access Points ermittelt wurden, wird ihnen standardmäßig der Autorisierungsstatus ? **Unbekannt** zugewiesen. Sie können den Status einzelner Gruppen von Access Points ändern, um deren Verhältnis zu Ihrem eigenen Netzwerk anzuzeigen, zum Beispiel „autorisiert“, „Nachbar?“ oder „Nicht autorisiert“.

  Sie haben auch die Möglichkeit, den Standard-Gerätestatus von ? **Unbekannt** auf ✓ **Autorisiert** zu ändern. Sobald die Änderung vorgenommen wurde, werden alle ermittelten Access Points als ✓ **Autorisiert** eingestuft. Sie können die Liste dann überprüfen und einzelnen Access Points einen entsprechenden individuellen Status zuweisen. Wenn Sie zum Beispiel wissen, dass ein bestimmter Access Point nicht autorisiert ist, können Sie ihm den Status **Markiertes Gerät** oder ⚠ **Nicht autorisiertes Gerät** zuweisen.

Um eine Standard-Geräteautorisierung festzulegen, wählen Sie **Tools > Standard-Geräteautorisierung (ACL) einstellen**.

Um einen Autorisierungsstatus für einen Access Point oder eine Gruppe von Access Points festzulegen, wählen Sie **Access Points** aus, markieren Sie einen Access Point, und drücken Sie dann F2 **ACL**.

Sie können für alle Access Points den Autorisierungsstatus ✓ **Autorisiert** festlegen, indem Sie ✓ **Alle APs auf „Autorisiert" setzen** auswählen. Dadurch werden alle ermittelten Access Points als ✓ **Autorisiert** gekennzeichnet. Bei dieser Vorgehensweise können Sie dann den Standard-Autorisierungsstatus auf ? **Unbekannt** einstellen und dadurch neu ermittelte Access Points als ? **Unbekannt** anzeigen. Das Anwenden dieser Methode ermöglicht ein schnelles Aufzeigen von Sicherheitsrisiken oder neuen Access Points.

Sie können auch eine AP-Serie basierend auf dem AP-Präfix „BSSID/MAC“ oder einem Hersteller-MAC-Präfix auf den Status „Autorisiert“ oder „Nicht autorisiert“ festlegen, indem Sie **AP-Serie auf „Autorisiert“ setzen** oder **AP-Serie auf „Nicht autorisiert“ setzen** auswählen. Mithilfe dieser Optionen können Sie beim Konfigurieren Zeit sparen und sich einen schnellen Überblick über mögliche Probleme verschaffen. Wenn beispielsweise die Richtlinien Ihres Netzwerks die Geräte eines bestimmten Herstellers verbieten, können Sie das Hersteller-MAC-Präfix verwenden, um die ACL auf „Nicht autorisiert“ einzustellen. Diese Access Points werden dann automatisch als „Nicht autorisiert“ angezeigt, sobald sie ermittelt wurden.

Hinweis

Wenn Sie Ihr Profil speichern, werden die zugeordneten ACLs ebenfalls als Teil dieses Profils gespeichert.

Der AutoTest enthält den optionalen Test „Nicht autorisierte Access Points“, durch den nicht autorisierte Access Points ermittelt und angezeigt werden. Um diese Funktion zu aktivieren, wählen Sie **Tools > Schwellenwerte/AutoTest-Einstellungen > AutoTest „Nicht autorisierte Access Points“**. Um exakte und aussagekräftige Testergebnisse zu erhalten, müssen Sie vor dem Ausführen des AutoTests Access-Point-ACLs (Authorization Control Lists) konfigurieren.

Wie kann ich einen Access Point orten?

Wählen Sie **Access Points** aus, wählen Sie einen Access Point aus und drücken Sie dann F2 **Orten** auf dem Bildschirm **Access-Point-Details**. Sie können auch die optionale externe Richtantenne von Fluke Networks verwenden, um Access Points schneller zu ermitteln.

Wie kann ich mein Netzwerk und meine Testsitzung dokumentieren?

Speichern Sie die Sitzung (💾 drücken), und verwenden Sie die AirCheck Manager-Software, um die Daten auf einen PC herunterzuladen und einen Bericht zu erstellen.

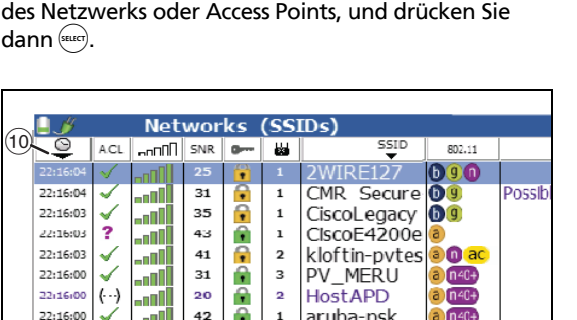
Wie kann ich alle Daten von meinem AirCheck löschen?

Wenn Sie alle Einstellungen, Sitzungsdaten und Profile vom Tester löschen möchten, wählen Sie **Tools > Alles löschen**. Dadurch werden alle Daten, die auf dem AirCheck-Tester gespeichert oder aufgezeichnet waren, gelöscht.

Finden von Kanälen, Netzwerken, APs oder Clients

Um Kanäle, Netzwerke, Access Points oder Clients zu finden, wählen Sie auf dem Startbildschirm entweder **Kanäle**, **Netzwerke, Access Points,** oder **Clients** aus. Die Abbildung 2 zeigt eine Liste der **Netzwerke**.

Zum Anzeigen der Details eines Netzwerks oder Access Points, verwenden Sie ▲ ▼ zum Markieren des Netzwerks oder Access Points, und drücken Sie dann SELECT.



gdp03a.eps

Abbildung 2. Liste der Netzwerke

① : der Zeitpunkt, zu dem das Netzwerk zum ersten Mal vom Tester wahrgenommen wurde. Zum Anzeigen von Netzwerken, die in Reichweite kommen, wenn Sie sich durch ein Gebiet bewegen, sortieren Sie die Liste absteigend entsprechend der Spalte „Zeitstempel“.

Drücken Sie , und bewegen Sie sich dann durch ein Gebiet. Netzwerke, die in Reichweite kommen, werden am Anfang der Liste angezeigt. Netzwerke, die nicht mehr in Reichweite sind, ändern ihre Farbe zu Grau, wenn **Nicht hörbare Access Points ausgrauen** aktiviert ist.

② **ACL:** der Autorisierungsstatus des Access Points. Der Standard-Status ist **? Unbekannt**, kann jedoch auf ✓ **Autorisiert** geändert werden. Ändern Sie den Status von jedem Access Point, um anzuzeigen, wie er sich zu Ihrem Netzwerk verhält. Um den Status zu ändern, wählen Sie auf dem Startbildschirm **Access Points** aus, wählen Sie einen Access Point aus, und drücken Sie dann F2 **ACL**.

(...): Nicht alle Access Points im Netzwerk haben denselben Autorisierungsstatus.

③ : die maximale Signalstärke aller Access Points für eine Netzwerk-SSID.

④ **SNR:** Das Signal to Noise Level (Signal-Rausch-Verhältnis) misst die Signalstärke im Verhältnis zu auftretenden Störungen. Das Verhältnis wird in Dezibel (dB) gemessen.

⑤ : der Sicherheitsstatus des Netzwerks:

Rotes geöffnetes Schloss: Das Netzwerk verfügt über keine aktivierte Sicherheit.

Hinweis

Zu einigen Netzwerken, für die ein offenes Schloss angezeigt wird, können Sie mit dem Tester eine Verbindung aufbauen und Messungen vornehmen, einschließlich dem Durchführen eines Ping-Tests. Möglicherweise können Sie aber zu demselben Netzwerk keine Verbindung mithilfe eines PCs aufbauen, um ohne Benutzer-ID und Kennwort Internetzugang zu erhalten.

Gelbes geschlossenes Schloss: Ein oder mehrere Access Points verwenden das WEP- oder Cisco-LEAP-Sicherheitsprotokoll. Diese sind weniger sicher als andere Protokolle.

Grünes geschlossenes Schloss: Alle Access Points verwenden Sicherheitsprotokolle, die sicherer sind als WEP, z. B. WPA oder WPA2.

(...): Die Access Points im Netzwerk verwenden nicht dasselbe Sicherheitsprotokoll. Ein Access Point verwendet möglicherweise WEP, während ein anderer vielleicht WPA verwendet.

⑥ : die Anzahl der vom Tester an Ihrem Standort wahrgenommenen Access Points.

⑦ **SSID**: Service Set Identifier. Der Name des WLANs.

: Das Netzwerk verfügt über Ad-hoc-Geräte. Dies sind Geräte, die Daten direkt mit anderen Geräten und nicht über Access Points austauschen. Ad-hoc-Geräte können Hackern Zugriff auf innerhalb des Netzwerks übertragene Daten geben. (Einige IT-Netzwerk-Richtlinien erlauben Ad-hoc-Geräte.)

[Unsichtbar]: Die SSID des Netzwerks wird nicht gesendet.

⑧ **802.11**: die 802.11-Standards, die die Access Points im Netzwerk verwenden:

802.11a: verwendet das 5 GHz-Band.

802.11b: verwendet das 2,4 GHz-Band.

802.11g: verwendet das 2,4 GHz-Band.

802.11n: verwendet das 2,4 GHz- oder das 5 GHz-Band.

802.11ac: verwendet das 5 GHz-Band.

Rote Balken: Der Tester hat einen Ländercode empfangen, der nicht mit der Einstellung unter **Tools** > **Land einstellen** übereinstimmt. Um festzustellen, aus welchem Netzwerk oder von welchem Access Point dieser Ländercode gesendet wird, wählen Sie **Netzwerke** oder **Access Points**, und suchen Sie dann nach den roten Balken in der Spalte **802.11**.

n40+ n40–: Ein oder mehrere Access Points verwenden einen verbundenen Kanal. Access Points, die den 802.11n-Standard verwenden, können einen Kanal mit einem Erweiterungskanal oberhalb (n40+) oder unterhalb (n40–) ihrer eigenen Frequenz anbinden, um einen 40-MHz-Kanal zu erzeugen. Dieser breitere Kanal ermöglicht dem Netzwerk einen höheren Durchsatz.

(...): Nicht alle Access Points im Netzwerk verwenden denselben 802.11-Standard.

⑨ **Notizen**: Drücken Sie ▷, um zum Feld „Notizen“ zu scrollen. Notizen werden vom Tester automatisch hinzugefügt. Netzwerke mit Notizen werden violett dargestellt.

(...): Für das Netzwerk existieren mehrere Notizen. Um alle Notizen anzuzeigen, markieren Sie das Netzwerk, und drücken Sie SELECT zweimal, um zum Bildschirm **Access-Point-Details** zu gelangen.

⑩ ▼▲: **Sortieren 1**, absteigende und aufsteigende Reihenfolge.

▼ ▲ : **Sortieren 2**, absteigende und aufsteigende Reihenfolge.

Um die Liste in aufsteigender oder absteigender Reihenfolge zu sortieren, verwenden Sie ▲▼ und ◀ ▶, um einen Spaltentitel zu markieren, und drücken Sie dann SELECT bzw. F1 **Sortieren 1**. Um beispielsweise rasch den Access Point mit dem stärksten Signal zu finden, markieren Sie ▁▃▅▇ oben in der Spalte, und drücken Sie dann SELECT bzw. F1 **Sortieren 1**. Dadurch wird der Access Point mit dem stärksten Signal ganz oben in der Liste angezeigt.

Um in einer zweitrangigen Reihenfolge zu sortieren, markieren Sie einen anderen Spaltentitel, und drücken Sie dann F2 **Sortieren 2**.

⑪ Drücken Sie F1 **Verbinden**, um eine Verbindung zum markierten Netzwerk herzustellen.

Die Schaltfläche „Verbinden“ wird als **Verbinden*** (mit einem Sternchen) angezeigt, wenn der Tester keine Verbindung mit dem markierten Netzwerk aufbauen kann. Um die Sicherheitseinstellungen für das Netzwerk zu konfigurieren, drücken Sie F1 **Verbinden***.

Hinweis

Um eine Verbindung mit einem geschützten Netzwerk aufzubauen, muss der Tester über ein Profil verfügen, das Sicherheitsanmeldeinformationen enthält. Verwenden Sie AirCheck Manager, um Sicherheitsanmeldeinformationen zu erstellen oder zu bearbeiten. Wenn Sie auf dem Tester auf ***Verbinden***** drücken, werden Sie durch die Sicherheitskonfiguration geführt. Sie können auch zuerst auf* ***Tools*** *drücken und dann auf* ***Profile verwalten/Netzwerk-Kennwörter****, um die Sicherheitseinstellungen zu konfigurieren. Das* ******* *auf der rechten Seite von* ***Verbinden*** *bedeutet, dass keine Sicherheitseinstellungen konfiguriert wurden. Informationen zum Einrichten von Sicherheitsrichtlinien finden Sie im Benutzerhandbuch.*

⑫

: der Kanal, der derzeit vom Tester überwacht wird. Die Farbe der Balken zeigt den Status des Ländercodes für die vorgeschriebene Domäne an.

⑬

: die Anzahl der Access Points, die an Ihrem Standort vom Tester wahrgenommen wurden. Dieser Wert schließt keine virtuellen Access Points mit ein, wenn **Virtuelle Access Points gruppieren** ausgewählt wurde.

⑭ Um die Beschreibungen der Symbole des Bildschirms **Netzwerke** anzuzeigen, drücken Sie F2 **Legende**.

Um Details der Access Points im Netzwerk anzuzeigen, verwenden Sie ▲ ▼ zum Markieren des Netzwerks, und drücken Sie dann SELECT.

FLUKE networks

AirCheck™
Testador Wi-Fi

Guia de Introdução

PN 3434814 12/2009 Rev. 4, 8/13 (Portuguese)
©2009-2013 Fluke Corporation. Printed in USA.
All product names are trademarks of their respective companies.
Wi-Fi® is a registered trademark of the Wi-Fi Alliance.

GARANTIA LIMITADA E LIMITAÇÃO DE RESPONSABILIDADE

A Fluke Networks garante que este produto não apresentará defeitos de materiais e fabricação por 1 (um) ano a partir da data da compra. As peças, acessórios, consertos e outros serviços são garantidos por 90 dias, a menos que indicado de outra forma. As baterias Ni-Cad, Ni-MH e Li-Ion, cabos ou outros periféricos são todos considerados peças e acessórios.

Esta garantia não cobre danos decorrentes de acidente, negligência, uso inadequado, alteração, contaminação ou condições anormais de operação ou manuseio. Os revendedores não estão autorizados a ampliar a garantia em nome da Fluke Networks.

Para obter um serviço durante o período de garantia, entre em contato com o Centro de assistência técnica autorizada da Fluke Networks mais próximo para obter informações de autorização de devolução. Depois, envie o produto para o Centro de assistência técnica com uma descrição do problema.

ESTA GARANTIA É O ÚNICO RECURSO DO COMPRADOR. NÃO É DADA NENHUMA OUTRA GARANTIA, TAL COMO GARANTIA DE ADEQUAÇÃO DO PRODUTO PARA DETERMINADO FIM, EXPRESSA OU IMPLÍCITA. A FLUKE NETWORKS NÃO SE RESPONSABILIZA POR NENHUM DANO OU PERDA, INCIDENTAL OU CONSEQUENTE, QUE POSSA OCORRER POR QUALQUER MOTIVO OU QUE SEJA DECORRENTE DE QUALQUER TEORIA JURÍDICA.

Como alguns estados ou países não permitem a exclusão ou limitação de uma garantia implícita, nem de danos incidentais ou consequentes, esta limitação de responsabilidade pode não ser aplicável no seu caso.

4/04

Fluke Networks
PO Box 777
Everett, WA 98206-0777
USA

Índice

Como acessar o Manual do Usuário..... 1
Informações de Atenção 2
Especificações gerais..... 5
Manutenção, Serviço e Proteção
do Equipamento contra falha..... 5
Para contatar a Fluke Networks 6
Carregamento e duração da bateria 7
Tela inicial 8
Configuração mínima para obter
o melhor desempenho 11
O que você pode saber sobre sua rede
sem fio?..... 12
O que é o funcionamento da minha rede? 12
O que há na LAN sem fio?..... 15
É possível conectar os dispositivos
à rede sem fio?..... 17
Qual é a causa de um desempenho lento
da rede e das quedas de conexão? 19
Existem riscos de segurança na rede?..... 20
Como posso Localizar um ponto de acesso?... 23
Como posso documentar minha rede
e minha sessão de teste? 23
Como posso apagar tudo no meu AirCheck?. 23
Descobrir Canais, Redes, PAs ou Clientes 24

Como acessar o Manual do Usuário

Este guia apresenta informações básicas para começar a usar o Testador AirCheck™ Wi-Fi. Para obter mais informações, consulte o Manual do Usuário no CD do Produto.

O CD também contém o AirCheck Manager para ajudá-lo a obter o máximo do testador.

Informações de Atenção

O Testador AirCheck ™ Wi-Fi é uma ferramenta portátil dedicada para verificar e solucionar problemas de redes Wi-Fi rapidamente.

⚠ Cuidado ⚠

Leia todas as informações de segurança antes de usar o produto.

Use o produto apenas como especificado, ou a proteção fornecida pelo produto pode ser comprometida.

Leia atentamente todas as instruções.

Use apenas adaptadores de energia aprovados pela Fluke para carregar a bateria.

Não use o produto em áreas próximas a gases explosivos, vapor ou em ambientes úmidos ou molhados.

Examine o caso antes de usar o produto. Verifique se existem rachaduras ou plástico faltando. Analise atentamente o isolamento ao redor dos terminais.

Baterias contêm produtos químicos perigosos que podem causar queimaduras ou explodir. Se ocorrer exposição aos produtos químicos, limpe com a água e obtenha ajuda.

Retire as baterias se o produto não for usado por um período prolongado de tempo, ou se for armazenado em temperaturas superiores a 50 °C. Se as baterias não forem removidas, o vazamento pode danificar o produto.

Não provoque curto nos terminais da bateria.

Não desmonte ou bate nas células de bateria e nos pacotes de baterias.

Não coloque as células da bateria os pacotes da bateria próximo ao calor ou fogo. Não coloque sob a luz solar.

Não carregue os pacotes da bateria continuamente quando não estiverem sendo usados.

Não exponha a bateria a choque mecânico.

Não abra a unidade da bateria. Não há peça interna que possa ser utilizada pelo usuário.

Consulte o manual do produto para obter instruções corretas para carregar a bateria

Para evitar risco de incêndio, choque elétrico, lesão física, danos ao equipamento ou inexatidão nos resultados de teste, leia as informações de segurança contidas no *Manual do usuário do AirCheck* antes de usar o testador.

	Atenção ou Cuidado: risco de dano ou destruição do equipamento ou do software. Veja as explicações no manual.
	Aviso: risco de choque elétrico.
	Produtos que contêm placas de circuitos não devem ser jogados no lixo comum. Informe-se sobre os procedimentos de descarte necessários de acordo com a regulamentação local.
	Este equipamento contém um rádio de Classe 2.
	Em conformidade com as normas relevantes da União Europeia
	Em conformidade com Regras FCC, Partes 15.107 e 15.109.

	Consta na relação da Canadian Standards Association.
	Conformidade com os padrões pertinentes da Austrália.
	Em conformidade com os Padrões de EMC relevantes da Coreia do Sul.

Informações adicionais sobre o Padrão de EMC da

A급 기기 **(업무용 방송통신기자재)**	이 기기는 업무용 **(A급)** 전자파 적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는 것을 목적으로 합니다.
Equipamento Classe A (Equipamento de Comunicação e Broadcasting Industrial)	Este equipamento é um equipamento industrial (Classe A) de adequação de ondas eletromagnéticas e o vendedor ou usuário deve estar ciente disso, e de que este equipamento deve ser usado em locais que sejam domicílios.

Especificações gerais

Tipo de bateria: bateria de lítio-íon removível recarregável (18,5 de horas)

Temperatura e umidade relativa de operação: 32 °F a 113 °F (0 °C a +45 °C)

Umidade relativa de operação: (% de umidade relativa sem condensação) 90% (50 °F a 95 °F; 10 °C a 35 °C) 75% (95 °F a 113 °F; 35 °C a 45 °C)

Armazenamento: -4 °F a 140 °F (-20 °C a 60 °C)

Impacto e vibração: Aleatórios, 2 g, 5 Hz a 500 Hz (Classe 2) teste de queda de 1 metro

Altitude: 4.000 m; Armazenamento: 12.000 m

Segurança: IEC/EN 61010-1

Manutenção, Serviço e Proteção do Equipamento contra falha

· A bateria é o único componente passível de manutenção pelo usuário. Não abra o produto, a não ser para substituir a bateria.

· Use apenas peças de reposição aprovadas pela Fluke Networks.

· Se este equipamento for usado de outra forma que não a especificada pelo fabricante, a proteção fornecida por ele poderá ser afetada.

· Limpe a parte externa da unidade com um pano macio umedecido com água ou água e detergente neutro.

Para contatar a Fluke Networks

www.flukenetworks.com

support@flukenetworks.com

+1-425-446-4519

- Austrália: 61 (2) 8850-3333 ou 61 (3) 9329 0244
- Pequim: 86 (10) 6512-3435
- Brasil: 11 3759 7600
- Canadá: 1-800-363-5853
- Europa: +31-(0) 40 2675 600
- Hong Kong: 852 2721-3228
- Japão: 03-6714-3117
- Coreia: 82 2 539-6311
- Singapura: +65-6799-5566
- Taiwan: (886) 2-227-83199
- E.U.A.: 1-800-283-5853

Visite nosso site para ver a lista completa de números de telefone.

Carregamento e duração da bateria

Carregue a bateria por 4 horas antes de usá-la pela primeira vez. Para carregar a bateria, conecte o adaptador CA ao conector de bateria no Testador AirCheck.

A duração da bateria é de aproximadamente 5,5 horas durante uma operação normal.

Exibe o estado da bateria. Quando a carga da bateria está fraca, o ícone pisca.

Mostra que o adaptador AC está conectado.

Tela inicial

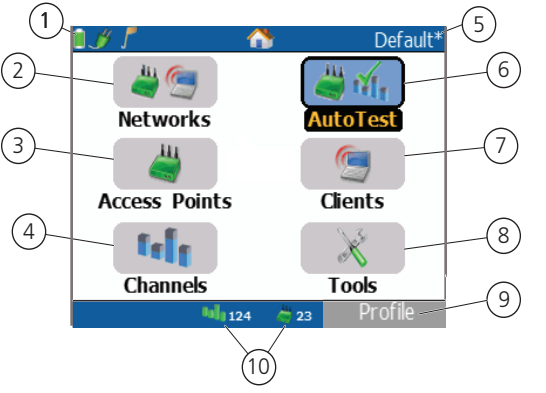


Figura 1. Componentes da Tela inicial

1

Exibe o estado da bateria. Quando a carga da bateria está fraca, o ícone pisca. Conecte o adaptador CA para carregar a bateria e assegurar que o testador continue a funcionar.

Mostra que o adaptador AC está conectado.

Indica que a antena externa está conectada.

Obs.:

O AirCheck não irá transmitir ou se conectar a um ponto de acesso quando a antena externa estiver conectada.

② **Redes**: Descobre LANs sem fio.

③ **Pontos de acesso**: Descobre pontos de acesso.

④ **Canais**: Indica a utilização de canais de WLAN.

⑤ O nome do perfil que o testador está usando no momento. O perfil é **Padrão** se um perfil diferente não tiver sido carregado. O nome tem um asterisco se tiver alterado uma configuração no testador desde que o perfil tenha sido carregado ou salvo.

⑥ **Autoteste**: verifica automaticamente o funcionamento da rede, ao observar a qualidade do ar (utilização dos canais e interferências), qualidade da rede (cobertura da rede e conectividade), e a presença de redes ad hoc. A detecção de ponto de acesso não autorizado é opcional e requer configuração de ACL.

⑦ **Clientes**: Descobre clientes que estão usando suas redes.

⑧ **Ferramentas**: Permite gerenciar arquivos e configurações.

⑨ **Perfil**: Exibe uma lista de perfis disponíveis.

⑩ À esquerda: o canal que o testador está monitorando no momento. A cor das barras exibe o estado do código do país de um domínio normativo. Um ícone vermelho pode indicar a operação de um canal ilegal da configuração de país atual e/ou a recepção de um código de país diferente.

À direita: o número de pontos de acesso físico ouvidos pelo testador.

Até 500 pontos de acesso podem ser armazenados no banco de dados de pontos de acesso no testador. Quando o ícone de ponto de acesso fica amarelo, indica que 400 ou mais pontos de acesso foram descobertos.

Quando o ícone fica vermelho, indica que 500 ou mais pontos de acesso foram descobertos e que o banco de dados de pontos de acesso está cheio. Nenhum novo ponto de acesso descoberto será incluído na lista.

Configuração mínima para obter o melhor desempenho

Alterar o idioma e a configuração do país

1 Selecione **Ferramentas**.

2 Para alterar o idioma das telas, selecione **Definir idioma**. Realce um idioma e pressione F2 **Salvar**.

3 Para alterar o país, selecione **Definir país**, selecione o país onde que será usado o testador e pressione F2 **Salvar**.

Para obter o melhor desempenho do testador, use o software AirCheck™ Manager para configurar um perfil e transferi-lo para o testador. Também pode-se configurar um perfil no Testador AirCheck testador e contém dados que permitem ao testador executar estas tarefas:

- Conectar a redes que requerem credenciais de segurança.
- Exibir o estado o status de autorização correto de cada ponto de acesso. Isso permite ver rapidamente quais pontos de acesso são partes autorizadas da rede.
- Executar o Ping nos principais dispositivos de rede.
- Execute um teste de conexão da porta TCP, por meio de um nome do host ou endereço IP e um número da porta designado.

O que você pode saber sobre sua rede sem fio?

O que é o funcionamento da minha rede?

- **Como é qualidade de ar de minha Wi-Fi? Meus canais estão sobrecarregados com pontos de acesso e tráfego Wi-Fi? Algum de meus canais é muito ruidoso?**

  Selecione **Autoteste**. Depois de executar o Autoteste, selecione **Qualidade do ar** para visualizar os resultados de Utilização do Canal 802.11, Não Utilização do Canal 802.11 e avaliar o funcionamento de interferência co-canal.

  Os resultados da Utilização de canal 802.11 incluem os três canais mais movimentados que tem mais tráfego Wi-Fi. O valor de utilização do canal é exibido junto com a classificação de ✓ Passar, ⚠ Atenção ou ✗ Falha. O grau de teste é baseado na comparação do valor real até limiares definidos pelo usuário. Esses limiares são configurados em **Ferramentas > Limiares / Configurações de Autoteste**.

  Utilização de canal valor junto com a classificação de passar, Aviso Falha, é apresentada. Os resultados de não Utilização de canal 802.11 incluem os três canais com maior não 802.11, interferência e ruído. O valor de utilização de canal é exibido junto com a classificação de ✓ Passar, ⚠ Atenção ou ✗ Falha.

Os resultados de interferência co-canal incluem os três principais canais com maiores PAs com uma intensidade de sinal e qualidade do sinal mínimas. A contagem de PA junto com a classificação em ou acima de ✓ Passar, ⚠ Atenção ou ✗ Falha é exibido.

- **Como está a qualidade da rede Wi-Fi? Posso ouvir quaisquer pontos de acesso que suportam minhas redes? Existem furos de cobertura nessa área? Há muitos PAs próximos utilizando o mesmo canal tornando minha rede lenta? Posso me contar?**

  Selecione **Autoteste** - Depois de executar o Autoteste, selecione **Qualidade da rede** para visualizar os resultados da Cobertura, Interferência co-canal, Segurança e avaliação do funcionamento da conexão.

  Os resultados de Cobertura incluem o número de pontos de acesso com boa qualidade de sinal, incluindo tanto boa intensidade de sinal quanto boa Razão Sinal-Ruído que suportam uma rede (SSID) junto com a classificação de ✓ Passar, ⚠ Atenção ou ✗ Falha são exibidos. O grau de teste é baseado em uma comparação dos valores reais até limiares definidos pelo usuário. Os limiares de contagem de PAs e qualidade de sinal de nível de sinal e sinal-ruído são definidos nas telas **Ferramentas > Limiares / Configurações de Autoteste > Cobertura de PA, Nível de sinal** e **Limiar sinal-ruído** .

A interferência co-canal e os resultados incluem o número de sobreposições de PAs de uma rede junto com a classificação de ✓ Passar, ⚠ Atenção ou ✗ Falha, com base em uma única comparação de rede com os limiares. Os limiares para esse teste são definidos na tela **Ferramentas > Limiares / Configurações de Autoteste > Limiares de co-canal de qualidade da rede**.

Os resultados de Segurança relatam se todos os PAs na SSID usam as mesmas credenciais de segurança junto com uma classificação de ✓ Passar, ⚠ Atenção ou ✗ Falha.

O teste de Conexão tenta se conectar a cada rede configurada em seu perfil. Os resultados do teste de Conexão indicam se é possível conectar-se a redes em seu local ou não com um grau de teste grau de Passar ou Falha. Detalhes adicionais sobre a conexão, por exemplo, canal, endereço IP recebido, taxa de conexão são fornecidos como uma classificação de ✓ Passar, ⚠ Atenção ou ✗ Falha.

- ❑ **Quais pontos de acesso não autorizados ou desconhecidos estão conectados à minha rede Wi-Fi?**
  Eles são um risco à segurança?

O teste de pontos de acesso não autorizados é uma parte opcional do Autoteste, ele indica se pontos de acesso não autorizados ou desconhecidos são detectados com uma classificação de ✔ Passar, ⚠ Atenção ou ✘ Falha. Os resultados incluem uma lista de todos os pontos de acesso não controlados ouvidos em seu local. A identificação de pontos de acesso não controlados requer a configuração de uma Lista de controle de acesso (ACL). A configuração da ACL está disponível na tela de Autoteste, ao selecionar **Pontos de acesso não controlados > ACL** ou **Início> Pontos de acesso > ACL**.

O que há na LAN sem fio?

- **Quais LANs sem fio estão disponíveis?**

  Selecione **Redes** para ver uma lista de LANs sem fio e os pontos de acesso que se conectam com cada rede. Para ver todos os pontos de acesso disponíveis em seu local, selecione **Pontos de acesso**.

- **Quais pontos de acesso estão disponíveis? As intensidades do sinal são suficientes?**

  Selecione **Pontos de acesso** para ver uma lista de pontos de acesso disponíveis em seu local e a intensidade do sinal dos pontos de acesso. Para ver os gráficos de barra da intensidade do sinal e ruído de um ponto de acesso, realce o ponto de acesso e depois pressione SELECT.

- ❑ **O ponto de acesso está configurado corretamente?**

  Na tela inicial, selecione **Pontos de acesso**, realce um ponto de acesso e depois pressione (SELECT).

- ❑ **Há novos pontos de acesso na área? Eles são seus pontos de acesso, de seus vizinhos ou de uma pessoa não autorizada?**

  Usar o recurso de status de autorização de dispositivo (ACL) para relatar automaticamente quando novos pontos de acesso forem localizados em seu local. Para usar esse recurso, configure status de autorização de ponto de acesso de cada ponto de acesso (por exemplo, autorizado ou vizinho), em seguida defina o status de autorização padrão de **? Desconhecido**. Consequentemente, o status de autorização padrão de **? Desconhecido** será atribuído a todos os pontos de acesso não descobertos anteriormente. Finalmente, selecione **Pontos de acesso** na tela inicial para ver todos os pontos de acesso marcados como **? Desconhecidos**.

  Alternativamente, salve a sessão de teste que contém a lista de pontos de acesso descobertos. Use o AirCheck Manager para comparar a lista de pontos de acesso com um arquivo de sessão salvo anteriormente para ver se foram descobertos pontos de acesso adicionais.

  Para especificar uma autorização de dispositivo padrão de desconhecido ou autorizado, selecione **Ferramentas > Definir padrão de autorização do dispositivo (ACL)**

❑ **Quais clientes sem fio usam a rede?**

Na tela inicial, selecione **Clientes**. Também é possível obter detalhes da PA ou do canal para ver a lista de clientes associados.

É possível conectar os dispositivos à rede sem fio?

Use o testador para verificar a conectividade.

❑ **É possível conectar um dispositivo como cliente à rede (SSID)?**

Selecione **Redes**, realce uma rede e pressione F1 **Conectar**.

Obs.:

Para conectar-se a uma rede segura, o testador deve ter um perfil que inclua credenciais de segurança.

❑ **É possível fazer um dispositivo se conectar a um ponto de acesso (BSSID)?**

Selecione **Pontos de acesso**, realce um ponto de acesso e depois pressione F1 **Conectar**. Se houver um ***** à direita de **Conectar**, significa que a segurança não foi configurada no testador para essa rede. Pressione **Conectar *** para ser orientado a entrar nas configurações de segurança. Quando terminar, as configurações serão salvas no perfil atual. Pressione **Ferramentas** e **Gerenciar perfis / senhas de rede** para reeditar as configurações de segurança se necessário.

- ❑ **Caso não seja possível conectar um dispositivo a uma rede ou ponto de acesso, onde estará a falha neste procedimento de conexão?**

  Veja o registro de conexão. Pressione F2 **Registro** da tela **Conectar à rede** ou **Conectar a ponto de acesso** .

- ❑ **É possível fazer com que um dispositivo execute um ping em um dispositivo de rede?**

  Faça um teste de ping. Conecte-se a uma rede ou ponto de acesso e, em seguida, pressione F1 **Iniciar testes**.

  Obs.:

  *Os destinos de ping podem ser adicionados ao selecionar **Ferramentas > Gerenciar perfis / senhas de rede > Editar destinos > Adicionar**. Pode-se acrescentar um destino com um endereço IP ou nome de host (URL).*

  *Se houver um ***** à direita de **Conectar**, significa que a segurança não foi configurada no testador para essa rede. Pressione **Conectar *** para ser orientado a entrar a entrar nas configurações de segurança.*

- ❑ **O cartão de interface de rede funciona corretamente em um cliente?**

  Selecione **Clientes**, e depois procure na coluna SSID. Os SSIDs tracejados estão investigando os clientes e os clientes com um nome de SSID exibido são clientes associados. Pressione SELECT para ver se o cliente transmite quadros de solicitações de sonda.

Qual é a causa de um desempenho lento da rede e das quedas de conexão?

- ❑ **A intensidade do sinal é suficiente?**

  Selecione **Pontos de acesso**. A tela **Pontos de acesso** mostra a intensidade do sinal de cada ponto de acesso. Selecione um ponto de acesso para ver mais detalhes sobre a intensidade e congestionamento do sinal.

- ❑ **A rede está muito ocupada?**

  Selecione **Canais** para ter uma visão geral de utilização do canal e do número de pontos de acesso que usam cada canal. Para ver um gráfico, realce o canal e pressione (SELECT).

- ❑ **Existe alguma interferência que não seja de 802.11 em algum canal?**

  Selecione **Canais**. Interferência que não a 802.11 é cinza. Esse ruído pode interferir nas conexões ou no desempenho da WLAN. O ruído que não seja o 802.11 pode ser gerado a partir dos fornos microondas, telefones sem fio, dispositivos Bluetooth®, detectores de movimento, câmeras sem fio e outros dispositivos sem fio.

Obs.:

As três medidas anteriores também estão resumidas no recurso ***Autoteste****.*

Existem riscos de segurança na rede?

- **As redes apresentam o nível esperado de segurança?**

  Selecione **Redes**. Redes que têm pontos de acesso inseguros exibem um cadeado vermelho ( ).

- **Existe alguma rede ad hoc na área?**

  Selecione **Redes**. Estações que estão em operação em modo de rede ad hoc serão marcadas com um ícone ad hoc ( ) na coluna SSID. Estações ad hoc podem representar riscos à segurança da rede ou violar suas políticas de rede.

  O Autoteste inclui um teste de rede Ad Hoc que sinaliza estações ad hoc.

- **Há pontos de acesso não autorizados na área? Onde estão?**

  O AirCheck pode ser usado para ajudar a localizar o status de autorização de pontos de acesso descobertos. Por definição padrão, quando são descobertos pontos de acesso, lhes é atribuído um status de autorização de ? **Desconhecido**. É possível alterar o status de indivíduo ou grupos de pontos de acesso para refletir sua relação com sua rede, por exemplo, autorizado, vizinho, não autorizado.

Também existe a opção de alterar o status do dispositivo padrão de ? **Desconhecido** para ✓ **Autorizado**. Uma vez alterado, todos os pontos de acesso descobertos serão identificados como ✓ **Autorizado**. É possível em seguida revisar a lista e atribuir status a pontos de acesso individuais adequadamente. Por exemplo, se você souber que um ponto de acesso não é autorizado, pode dar a ele um o status de **Dispositivo sinalizado** ou ⚠ **Dispositivo não autorizado**.

Para especificar uma autorização de dispositivo padrão, selecione **Ferramentas > Definir padrão de autorização de dispositivo (ACL)**.

Para atribuir um status de autorização a um ponto de acesso ou grupo de pontos de acesso, selecione **Pontos de acesso**, realce um ponto de acesso e pressione F2 **ACL**.

É possível definir o status de autorização de todos os pontos de acesso para ✓ **Autorizado** ao selecionar ✓ **Definir todos os PAs como Autorizados**. Isso fará com que todos os pontos de acesso sejam marcados como ✓ **Autorizado**. Usando essa abordagem, quando o status de autorização padrão for, em seguida, definido para ? **Desconhecido**, pontos de acesso recém-descobertos serão como ? **Desconhecido**. Em geral, esse método fornecerá visibilidade rápida dos riscos de segurança ou novos pontos de acesso.

Também é possível definir uma série de PAs para autorizado ou não autorizado com base no AP BSSID/MAC ou no prefixo MAC do fornecedor, ao selecionar **Definir série PA para Autorizado** ou **Definir série PA para Não autorizado**. Essas opções podem reduzir o tempo gasto na configuração e fornecer visibilidade rápida de possíveis problemas. Por exemplo, se o equipamento de um fornecedor específico não tem permissão por sua política de rede, use o prefixo MAC do fornecedor para definir a ACL para não autorizado. Quando esses pontos de acesso são detectados, serão automaticamente encaminhados como não autorizados.

Obs.:

Quando você salva seu perfil, as ACLs designadas também serão salvas como parte desse perfil.

O autoteste inclui opcionalmente Teste de Ponto de Acesso Não Autorizado que detecta e relata pontos de acesso não autorizados. Para habilitar esta funcionalidade, vá para **Ferramentas > Limiares/ Configurações de Autoteste > Autoteste de pontos de acesso não autorizados**. Para resultados de testes precisos e significativos, é necessário configurar pontos de acesso das ACLs antes de executar o autoteste.

Como posso Localizar um ponto de acesso?

Selecione **Pontos de acesso**, selecione um ponto de acesso e depois pressione F2 **Localizar** na tela **Detalhes de ponto de acesso**. Também é possível usar a antena direcional externa da Fluke Networks opcional para ajudar a encontrar seus pontos de acesso mais rapidamente.

Como posso documentar minha rede e minha sessão de teste?

Salve a sessão (pressione 💾), depois use o software do AirCheck Manager para baixar os dados em um computador e gerar o relatório.

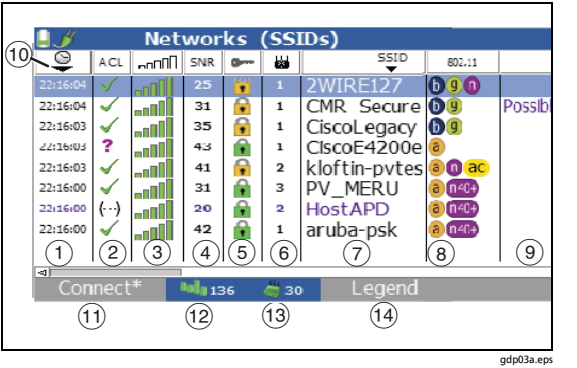
Como posso apagar tudo no meu AirCheck?

Se quiser apagar todas as configurações, os dados da sessão e de perfis do testador, selecione **Ferramentas > Apagar tudo** - tudo o que foi salvo ou armazenado no Testador AirCheck é apagado.

Descobrir Canais, Redes, PAs ou Clientes

Para descobrir canais, redes, pontos de acesso ou clientes, selecione **Canais**, **Redes, Pontos de acesso,** ou **Clientes** da tela inicial. A figura 2 exibe uma lista de **Redes**.

Para ver detalhes sobre uma rede ou um ponto de acesso, use ▲ ▼ para realçar a rede ou o ponto de acesso e, em seguida, pressione SELECT.



gdp03a.eps

Figura 2. Lista de redes

① : o momento em que o testador ouviu a rede pela primeira vez. Para ver redes que entram na faixa de alcance conforme você navega por uma área, ordene a lista em uma sequência decrescente da coluna do registro de hora.

Pressione , em seguida, navegue por uma área. As redes que entram na faixa de alcance são adicionadas ao topo da lista. As redes que ficam fora do intervalo tornam-se cinzas se **Pontos de acesso não audíveis cinzas** estiver ativado.

② **ACL**: O status de autorização do ponto de acesso. O status padrão é ? **Desconhecido**, mas pode ser alterado para ✓ **Autorizado**. Altere o status de cada ponto de acesso para exibir como ele está relacionado com sua rede. Para alterar o status, selecione **Pontos de acesso** da tela inicial, selecione um ponto de acesso e depois pressione F2 **ACL**.

(...): Todos os pontos de acesso na rede não têm o mesmo status de autorização.

③ : A intensidade máxima do sinal de todos os pontos de acesso de uma rede SSID.

④ **SNR**: Nível de sinal-ruído é uma medida de intensidade do sinal em relação ao ruído. A razão é medida em decibéis (dB).

⑤ : O status de segurança da rede:

Cadeado vermelho aberto: A segurança não está habilitada na rede.

Obs.:

Algumas redes com um cadeado aberto permitirão que você conecte o testador e executar medições incluindo a execução do teste de Ping, mas podem não permitir que um computador conecte-se à mesma rede para se conectar à web sem um ID de usuário e uma senha.

Cadeado amarelo fechado: um ou mais pontos de acesso usam os protocolos de segurança WEP ou LEAP da Cisco. Estes protocolos são menos seguros que outros.

Cadeado verde fechado: Todos os pontos de acesso utilizam protocolo de segurança que são mais seguros que o WEP, como por exemplo, WPA ou WPA2.

(...): os pontos de acesso da rede não utilizam todos o mesmo tipo de segurança. Por exemplo, um utiliza WEP e outro, WPA.

⑥ : O número de pontos de acesso que o testador detecta em seu local.

⑦ **SSID**: Service Set Identifier. O nome da rede sem fio.

: A rede tem dispositivos ad hoc. Esses dispositivos comunicam-se diretamente com outros dispositivos, não por meio de um ponto de acesso. Os dispositivos ad hoc podem oferecer aos hackers o acesso a dados transmitidos pela rede. (Algumas políticas de TI para redes permitem dispositivos ad hoc.)

[Oculto]: A rede não transmite o seu SSID.

⑧ **802.11**: Os padrões 802.11 que os pontos de acesso usam na rede:

a 802.11a: Usa a banda 5 GHz.

b 802.11b: Usa a banda 2,4 GHz.

g 802.11g: Usa a banda 2,4 GHz.

n 802.11n : Usa a banda 2,4 GHz ou 5 GHz.

ac 802.11ac: Usa a banda 5 GHz.

Barras vermelhas: o testador recebeu um código de país que é diferente da configuração em **Ferramentas** > **Defina país**. Para identificar a rede ou o ponto de acesso que transmite o código, selecione **Redes** ou **Pontos de acesso**, depois procure as barras vermelhas na coluna **802.11**.

n40+ n40-: um ou mais pontos de acesso utilizam um canal vinculado. Pontos de acesso que usam o padrão 802.11n podem vincular um canal a um canal de extensão acima (n40+) ou abaixo dele (n40-) para fazer um canal de 40 MHz. Esse canal mais largo fornece à rede um maior rendimento.

(...): Todos os pontos de acesso na rede não usam o mesmo padrão 802.11.

⑨ **Notas**: Pressione ▷ para rolar o campo de notas. O testador adiciona notas automaticamente. As redes que têm notas são mostradas em roxo.

(...): a rede tem várias notas. Para ver todas as notas, realce a rede e pressione SELECT duas vezes para ir para a tela **Detalhes dos pontos de acesso**.

⑩ : **Classif 1**, sequências decrescentes e crescentes.

: **Classif 2**, sequências decrescentes e crescentes.

Para colocar a lista em ordem crescente ou decrescente, use e para realçar o título de uma coluna e pressione ou **Classif 1**. Por exemplo, para localizar rapidamente o ponto de acesso que possui o sinal mais forte, realce na parte superior da coluna e pressione ou **Classif 1**. Isso coloca o ponto de acesso com o sinal mais forte no topo da lista.

Para classificar em uma sequência secundária, realce um cabeçalho de coluna diferente, depois pressione **Classif 2**.

⑪ Pressione **Conectar** para conectar-se à rede realçada.

O botão de conexão é exibido como **Conectar*** (com um asterisco) se o testador não conseguir se conectar à rede realçada. Para estabelecer as configurações de segurança da rede, pressione **Conectar***.

Obs.:

Para se conectar uma rede segura, o testador deve ter um perfil que inclua credenciais de segurança. Crie ou edite credenciais de segurança no testador ou com o AirCheck Manager. Ao pressionar ***Conectar***** no testador, ele o encaminhará pela configuração de segurança. Também é possível pressionar* ***Ferramentas*** *e* ***Gerenciar perfis /senhas de rede*** *para reconfigurar as configurações de segurança. O* ******* *à direita de* ***Conectar*** *indica que nenhuma definição de segurança foi configurada. Consulte o Manual do usuário para configurar os procedimentos de segurança usando Conectar.*

⑫

: o canal que o testador monitora no momento. A cor das barras mostra o status do código do país de um domínio normativo.

⑬

: o número de pontos de acesso que o testador ouve em seu local. Esse número não inclui pontos de acesso virtuais se **Agrupar pontos de acesso virtuais** estiver selecionado.

⑭ Para ver as descrições dos ícones na tela **Redes**, pressione F2 **Legenda**.

Para ver detalhes sobre os pontos de acesso em uma rede, use ▲ ▼ para realçar uma rede, depois pressione SELECT.

FLUKE networks

AirCheck™

WiFi-тестер

Руководство по началу работы с устройством

PN 3434814 12/2009 Rev. 4, 8/13 (Russian)
©2009-2013 Fluke Corporation. Printed in USA.
All product names are trademarks of their respective companies.
Wi-Fi® is a registered trademark of the Wi-Fi Alliance.

ОГРАНИЧЕННАЯ ГАРАНТИЯ И ОГРАНИЧЕНИЯ ОТВЕТСТВЕННОСТИ

Fluke Networks гарантирует, что данный продукт не имеет дефектов в материалах и качестве изготовления на срок один год с даты продажи. Для деталей, аксессуаров, ремонта продукта и его обслуживания устанавливается гарантийный срок 90 дней, если не указано иное. Никель-кадмиевые, никель-металлогидридные и литий-ионные аккумуляторы, кабели и другое периферийное оборудование также считаются деталями и аксессуарами.

Данная гарантия не предусматривает возмещения ущерба, возникшего вследствие случайного повреждения, небрежного или ненадлежащего обращения, внесения изменений, загрязнения либо эксплуатации или обслуживания в непредусмотренных условиях. Торговый представитель не обладает правом предоставлять какие-либо другие гарантии от лица компании Fluke Networks.

Для получения информации об обслуживании оборудования в течение гарантийного периода обратитесь в ближайший авторизованный сервисный центр Fluke Networks, затем отправьте неисправное изделие в данный сервисный центр с описанием неполадки.

ДАННАЯ ГАРАНТИЯ ЯВЛЯЕТСЯ ВАШИМ ЕДИНСТВЕННЫМ СРЕДСТВОМ ЗАЩИТЫ ПРАВ. НЕ ПРЕДОСТАВЛЯЕТСЯ В ЯВНОМ ВИДЕ И НЕ ПОДРАЗУМЕВАЕТСЯ НИКАКИХ ДРУГИХ ГАРАНТИЙ, НАПРИМЕР, В ОТНОШЕНИИ ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОГО НАЗНАЧЕНИЯ. FLUKE NETWORKS НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ НИ ЗА КАКИЕ ОСОБЫЕ, КОСВЕННЫЕ, СЛУЧАЙНЫЕ ИЛИ ПРОИСТЕКАЮЩИЕ УБЫТКИ ИЛИ УЩЕРБ, КОТОРЫЕ МОГУТ ВОЗНИКНУТЬ ПО КАКОЙ-ЛИБО ПРИЧИНЕ ИЛИ ТЕОРЕТИЧЕСКИ.

Поскольку в некоторых странах и штатах запрещено ограничение условий подразумеваемой гарантии или исключение и ограничение случайных и косвенных убытков, то ограничения и исключения настоящей гарантии в этих случаях могут не применяться.

4/04

Fluke Networks
PO Box 777
Everett, WA 98206-0777
USA

Содержание

Доступ к Руководству пользователя 1
Предупреждения 2
  Общие характеристики 5
  Содержание, обслуживание и защита оборудования от повреждений 6
Fluke Networks, контактная информация 7
Зарядка и продолжительность работы батареи 8
Главный экран 9
Минимальная конфигурация для обеспечения наилучшей производительности тестера 12
Что можно узнать о вашей беспроводной сети 13
  Какова степень исправности сети? 13
  Что содержит беспроводная локальная сеть? 18
  Могут ли устройства подключаться к беспроводной сети? 20
  Каковы причины низкой производительности сети или обрыва связи? 22
  Существуют ли в сети угрозы безопасности? 23
  Как можно определить местоположение точки доступа? 26
  Как составить документ с результатами тестового сеанса и проверки сети? 26

Как удалить всю информацию из AirCheck? 26
Обнаружение каналов, сетей, точек доступа или клиентов.....27

Доступ к Руководству пользователя

Данное руководство содержит базовые сведения, которые помогут вам начать пользоваться Wi-Fi-тестером AirCheck™. За дополнительной информацией обращайтесь к руководству пользователя на компакт-диске из комплекта продукта.

На этом же компакт-диске находится приложение AirCheck Manager, которое поможет максимально эффективно использовать тестер.

Предупреждения

Wi-Fi-тестер AirCheck™ является специализированным ручным инструментом для быстрой проверки сетей Wi-Fi и поиска неисправностей в них.

⚠Предупреждение⚠

Перед использованием Продукта ознакомьтесь с информацией о безопасности.

Используйте Продукт только по назначению; в противном случае полная функциональность устройства не гарантируется.

Внимательно прочитайте все инструкции.

Для подзарядки аккумуляторных батарей используйте только адаптеры переменного тока, одобренные Fluke Networks.

Запрещается эксплуатация Продукта, если в окружающей атмосфере присутствует пар или взрывоопасные газы, а также в условиях повышенной влажности.

Перед использованием внимательно осмотрите корпус Продукта. Убедитесь в отсутствии трещин, отколовшегося пластика, а также повреждений изоляции вокруг контактов.

Батареи содержат опасные взрывчатые химические вещества, воздействие которых может вызвать ожоги. В случае получения травм смойте химикаты водой и обратитесь к врачу.

Если Продукт не используется в течение длительного периода времени или хранится при температуре выше 50 °C, из него следует извлечь батареи. В противном случае химические вещества, вытекшие из батарей, могут повредить Продукт.

Не замыкайте контакты батареи.

Не разбирайте и не разрушайте батареи и составляющие их элементы.

Не располагайте батареи и составляющие их элементы рядом с источником тепла или открытым огнем. Не подвергайте батареи воздействию прямых солнечных лучей.

Не оставляйте батареи на постоянной подзарядке, если Продукт не используется.

Не подвергайте батареи воздействию механических ударов.

Не вскрывайте батареи; внутри не содержится компонентов, требующих обслуживания пользователем.

Необходимые инструкции по подзарядке батареи приводятся в руководстве пользователя Продукта.

Во избежание пожара, поражения электрическим током, получения травмы, повреждения оборудования или получения неточных результатов измерения ознакомьтесь с информацией о мерах предосторожности в *Руководстве пользователя AirCheck перед* использованием тестера.

	Предупреждение или предостережение. Опасность повреждения или уничтожения оборудования или программного обеспечения. См. пояснения в руководстве.
	Предупреждение. Угроза поражения электрическим током.
	Запрещается выбрасывать продукты, содержащие печатные платы, в мусорные контейнеры. Процедуры утилизации определяются местными нормативными актами.
	Это оборудование содержит радиоустройства класса 2.
	Соответствует требованиям директив Европейского Союза.
	Соответствует Правилам FCC, части 15.107, 15.109.
	Соответствует требованиям Канадской ассоциации стандартов (Canadian Standards Association).
	Соответствует требованиям стандартов Австралии

	Соответствует надлежащим стандартам Южной Кореи по электромагнитной совместимости.

Дополнительная информация о стандартах Южной Кореи по электромагнитной совместимости:

Электромагнитная совместимость. Применяется только при использовании в Южной Корее. Оборудование класса A (Промышленное оборудование для связи и радиовещания) [1]	[1] Данный продукт соответствуют стандартам промышленного (класс A) электромагнитного оборудования, и продавец или пользователь должны иметь это в виду. Данное оборудование предназначено для использования в промышленной среде. Его применение в домашних условиях запрещено.

Общие характеристики

Тип аккумулятора: съемная литий-ионная аккумуляторная батарея (18,5 Вт-ч)

Рабочая температура и относительная влажность: от 0 до +45 ºC (от 32 до 113 ºF)

Рабочая относительная влажность: (% без конденсации) 90 % (от 10 до 35 ºC; от 50 до 95 ºF) 75 % (от 35 до 45 ºC; от 95 до 113 ºF)

Хранение: от 20 до +60 ºC (от -4 до 140 ºF)

Удары и вибрации: стохастические, 2 g, 5-500 Гц (класс 2), прошел тест на удар при падении с высоты 1 м

Предельная высота: 4000 м; хранение: 12 000 м

Безопасность: IEC/EN 61010-1

Содержание, обслуживание и защита оборудования от повреждений

- Единственным компонентом, обслуживаемым пользователем, является аккумуляторная батарея. Не открывайте корпус для других целей, кроме замены аккумулятора.
- Используйте только те запчасти, которые одобрены Fluke Networks.
- Если данный прибор используется не по назначению, то он может не обеспечивать указанный класс защиты.
- Для очистки корпуса используйте мягкую ткань, смоченную водой или водой и мягкодействующим моющим средством.

Fluke Networks, контактная информация

www.flukenetworks.com

support@flukenetworks.com

+1-425-446-4519

- Австралия: 61 (2) 8850-3333 или 61 (3) 9329 0244
- Пекин: 86 (10) 6512-3435
- Бразилия: 11 3759 7600
- Канада: 1-800-363-5853
- Европа: +31-(0) 40 2675 600
- Гонконг: 852 2721-3228
- Япония: 03-6714-3117
- Корея: 82 2 539-6311
- Сингапур: +65-6799-5566
- Тайвань: (886) 2-227-83199
- США: 1-800-283-5853

Для того чтобы посмотреть полный список телефонных номеров, посетите наш веб-сайт.

Зарядка и продолжительность работы батареи

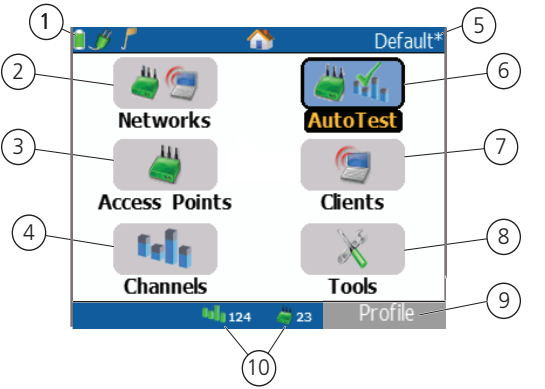
Перед первым использованием зарядите аккумулятор в течение 4 часов. Для зарядки аккумулятора подключите к разъему аккумулятора на тестере AirCheck адаптер питания переменного тока.

Продолжительность работы батареи - приблизительно 5,5 часов в нормальных условиях.

Показывает состояние аккумулятора. При низком заряде аккумулятора значок начинает мигать.

Показывает, что подключен адаптер питания переменного тока.

Главный экран



Home.eps

Рис. 1. Элементы главного экрана

1

Показывает состояние аккумулятора. При низком заряде аккумулятора значок мигает. Для зарядки аккумулятора и обеспечения дальнейшей работы тестера подключите к разъему аккумулятора адаптер питания переменного тока.

Показывает, что подключен адаптер питания переменного тока.

Показывает, что подсоединена внешняя антенна.

Примечание

С подсоединенной внешней антенной AirCheck не выполняет передачу и не подключается к точке доступа.

② **Сети.** Обнаружение беспроводных локальных сетей.

③ **Точки доступа.** Обнаружение точек доступа.

④ **Каналы.** Отображение используемых каналов беспроводной сети.

⑤ Имя профиля, которое в данный момент используется тестером. Если ранее не был загружен другой профиль, используется профиль **По умолчанию.** Рядом с именем отображается звездочка, если с момента последней загрузки или сохранения профиля настройка в тестере была изменена.

⑥ **Автотест.** Автоматическая проверка исправности сети путем наблюдения за качеством эфира (использование каналов и помехи), качеством сети (покрытие сети и возможность подключения) и наличием сетей "ad hoc". Обнаружение несанкционированных точек доступа является дополнительной возможностью и требует настройки списков контроля доступа.

⑦ **Клиенты.** Обнаружение клиентов, использующих ваши сети.

⑧ **Инструменты.** Возможность управления файлами и настройками.

⑨ **Профиль.** Показ списка доступных профилей.

⑩ Слева. Канал, который в данный момент отслеживается тестером. Цвет полосок показывает состояние кода страны для управляющего домена. Значок красного цвета может указывать на использование канала, являющегося запрещенным для заданной в данный момент страны, и/или на прием другого кода страны.

Справа. Количество физических точек доступа, обнаруженных тестером.

В базе данных точек доступа в тестере может храниться до 500 точек доступа. Желтый цвет значка точки доступа указывает, что обнаружено 400 или более точек доступа.

Красный цвет значка точки доступа указывает, что обнаружено 500 или более точек доступа и база данных точек доступа заполнена. Все новые обнаруженные точки доступа не попадут в список.

Минимальная конфигурация для обеспечения наилучшей производительности тестера

Изменение настроек языка и страны

1. Выберите меню **Инструменты**.
2. Для смены языка на экранах выберите **Установить язык**. Выделите язык и нажмите F2 **Сохранить**.
3. Чтобы изменить страну, выберите **Установить страну**, выберите страну, где вы будете использовать тестер, и нажмите F2 **Сохранить**.

Для использования тестера с максимальной эффективностью воспользуйтесь программой AirCheck™ Manager для настройки профиля и загрузки его в тестер. Профиль можно настроить
и в самом тестере AirCheck. Профиль содержит данные, которые позволяют с помощью тестера выполнять следующие задачи:

- Подключение к сети, в которой требуются регистрационные данные безопасности.
- Отображение корректного состояния авторизации для каждой точки доступа. Он позволяет оперативно визуально определять, какие из точек доступа являются авторизованными частями сети.
- Проверка доступности основных сетевых устройств с помощью запроса ping.
- Запустите тест подключения через порт TCP, используя имя хоста или IP-адрес и назначенный номер порта.

Что можно узнать о вашей беспроводной сети

Какова степень исправности сети?

- **Каково качество радиоэфира для передачи сигнала Wi-Fi?**
  Перегружены ли каналы при данном количестве точек доступа и трафике Wi-Fi?
  Не присутствует ли в части каналов чрезмерный шум?

  Выберите **Автотест**. После выполнения проверки **Автотест** выберите **Качество связи**, чтобы просмотреть результаты использования каналов с учетом факторов 802.11, использования каналов с учетом других факторов помимо 802.11 и оценку состояния внутриканальных помех.

  Результаты измерения загрузки каналов с учетом факторов 802.11 включают в себя три наиболее занятых канала, через которые проходит наибольший трафик Wi-Fi. Отображается значение загрузки канала, а также оценка прохождения теста: ✓ тест прошел, ⚠ предупреждение или ✗ тест не прошел. Оценка теста основана на сравнении фактического значения с установленной пользователем пороговой величиной. Пороговые величины задаются через меню **Инструменты > Пороговые значения / Настройки автотеста**.

Результаты измерения загрузки каналов с учетом других факторов помимо 802.11 включают в себя три канала с наибольшими помехами и шумом, источниками которых не являются устройства 802.11. Отображается значение загрузки канала, а также оценка прохождения теста: ✓ тест прошел, ⚠ предупреждение или ✗ тест не прошел.

Результаты оценки внутриканальных помех включают в себя три канала с наибольшим количеством точек доступа, имеющих минимальный уровень сигнала и самое низкое качество сигнала. Отображается количество точек доступа, а также оценка в сравнении с уровнями ✓ тест прошел, ⚠ предупреждение и ✗ тест не прошел.

- **Каково качество моей сети Wi-Fi?**
  Можно ли уловить сигнал от точек доступа, которые обеспечивают поддержку моей сети?
  Наблюдаются ли мертвые зоны покрытия?
  Не чрезмерна ли плотность точек доступа, использующих один и тот же канал, что замедляет работу сети?
  Возможно ли установить соединение?

  Выберите **Автотест** — после выполнения **Автотест** выберите **Качество сети** для просмотра результатов оценки покрытия, внутриканальных помех, безопасности и надежности соединения.

Результаты оценки покрытия включают в себя количество точек доступа с высоким качеством сигнала, что подразумевает как высокий уровень сигнала, так и хорошее отношение сигнал/шум, обеспечивающих поддержку сети (SSID), отображается также оценка прохождения теста: ✓ тест прошел, ⚠ предупреждение или ✗ тест не прошел. Оценка теста основана на сравнении фактических значений с установленными пользователем пороговыми величинами. Количество точек доступа и пороговые величины уровня сигнала и отношения сигнал/шум для оценки качества сигнала устанавливаются на экранах **Инструменты > Пороговые значения / Настройки автотеста > Покрытие точками доступа, Уровень сигнала** и **Пороговое отношение сигнал/шум**.

Результаты оценки внутриканальных помех содержат количество точек доступа сети, имеющих перекрывающиеся зоны, а также оценку прохождения теста — ✓ тест прошел, ⚠ предупреждение или ✗ тест не прошел — на основании сравнения с пороговыми величинами для одиночной сети. Пороговые величины для этого теста задаются на экране **Инструменты > Пороговые значения / Настройки автотеста > Внутриканальные пороговые значения для оценки качества сети**.

Результаты оценки безопасности показывают, все ли точки доступа с данным SSID используют одинаковые регистрационные данные безопасности, а также оценку прохождения теста: ✓ тест прошел, ⚠ предупреждение или ✗ тест не прошел.

В ходе выполнения теста на установку соединения выполняется попытка подключения к каждой сети, настроенной в профиле. Результаты теста на установку соединения показывают, возможно ли установить соединение с сетями из текущего местоположения, показывая результат как "тест прошел" или "тест не прошел". Предоставляются также дополнительные сведения о соединении, например, канал, полученный IP-адрес, скорость соединения, оценка которых представлена как ✔ тест прошел, ⚠ предупреждение или ✘ тест не прошел.

- **Какие неавторизованные или неизвестные точки доступа подключены к данной сети Wi-Fi? Существуют ли угрозы безопасности?**

  Проверка на наличие несанкционированных точек доступа является дополнительной частью Автотест, она показывает, обнаружены ли неавторизованные или неизвестные точки доступа в виде показания ✔ тест прошел, ⚠ предупреждение или ✘ тест не прошел. В результаты входит список всех несанкционированных точек доступа, обнаруженных из данного местоположения. Для выявления несанкционированных точек доступа требуется настройка списка контроля доступа (ACL). Настройку ACL можно выполнить на экране "Автотест", выбрав **Несанкционированные точки доступа > ACL** или **Главная > Точки доступа > ACL**.

Что содержит беспроводная локальная сеть?

- **Какие беспроводные локальные сети доступны?**

  Выберите **Сети** для просмотра списка беспроводных локальных сетей и точек доступа, подключенных к каждой из сетей. Для просмотра всех точек доступа, доступных в данном местоположении, выберите **Точки доступа**.

- **Какие точки доступа доступны? Достаточны ли уровни сигнала?**

  Выберите **Точки доступа** для просмотра списка точек доступа, доступных в данном местоположении, и уровней сигнала этих точек доступа. Для просмотра гистограмм уровней сигнала и шума для отдельной точки доступа выделите эту точку доступа и нажмите SELECT.

- **Точка доступа настроена корректно?**

  На главном экране выберите **Точки доступа**, выделите точку доступа и нажмите SELECT.

- **Имеются ли на данном участке точки доступа? Принадлежат ли они вашим сетям, соседним сетям или являются несанкционированными?**

Используйте функцию авторизации устройства (ACL) для автоматического создания отчета при обнаружении новых точек доступа в данном местоположении. Чтобы воспользоваться этой функцией, настройте состояние авторизации точек доступа для каждой точки доступа (например, авторизованная или соседняя), затем установите состояние авторизации по умолчанию как ? **Неизвестно**. В результате состояние авторизации ? **Неизвестно** будет присваиваться любым точкам доступа, которые не были обнаружены ранее. В завершение выберите **Точки доступа** на главном экране для просмотра всех точек доступа, имеющих состояние ? **Неизвестно**.

Другим способом является сохранение сеанса проверки, который содержит список обнаруженных точек доступа. С помощью AirCheck Manager сравните список точек доступа с ранее сохраненным файлом сеанса, чтобы проверить, не обнаружены ли дополнительные точки доступа.

Для задания состояния авторизации по умолчанию для устройств как "неизвестно" или "авторизованное", выберите **Инструменты > Установить авторизацию устройств по умолчанию (ACL)**

- **Какие клиентские устройства беспроводной связи используют сеть?**

  На главном экране выберите **Клиенты**. Можно также перейти на уровень сведений о точке доступа или канала, чтобы просмотреть список связанных клиентов.

Могут ли устройства подключаться к беспроводной сети?

Используйте тестер для проверки возможности соединения.

- ❑ **Может ли устройство подключиться к сети (SSID) в качестве клиента?**

  Выберите **Сети**, выделите сеть и нажмите F1 **Подключить**.

  Примечание

  Для подключения к защищенной сети тестер должен иметь профиль, содержащий регистрационные данные безопасности.

- ❑ **Может ли устройство подключиться к точке доступа (BSSID)?**

  Выберите **Точки доступа**, выделите точку доступа, затем нажмите F1 **Подключить**. Наличие звездочки (*) справа от элемента **Подключить** указывает на то, что для этой сети в тестере не настроены параметры безопасность. Нажмите **Подключить*** — будет запущена процедура ввода настроек безопасности. После ее завершения настройки сохраняются в текущем профиле. Если потребуется изменить настройки безопасности, нажмите **Инструменты**, затем нажмите **Управление профилями / паролями сети**.

- ❑ **Если устройство не может соединиться с сетью или с точкой доступа, где происходит сбой процедуры подключения?**

Просмотрите журнал соединений. Нажмите F2 **Журнал**, когда находитесь на экране **Подключение к сети** или **Подключение к точке доступа.**

- **Может ли устройство отправить запрос ping на сетевое устройство?**

  Выполняется тестовая передача пакетов Ping. Подключитесь к сети или точке доступа и нажмите F1 **Запустить тесты**.

  Примечание

  *Адресатов пакетов Ping можно добавить, выбрав **Инструменты > Управление профилями / паролями сети > Редактировать адресатов > Добавить**. Адресата можно добавить по его IP-адресу или по имени хоста (URL).*

  *Наличие звездочки (*) справа от элемента **Подключить** указывает на то, что для этой сети в тестере не настроены параметры безопасности. Нажмите **Подключить*** — будет запущена процедура ввода настроек безопасности.*

- **Правильно ли работает сетевая карта в клиенте?**

  Выберите **Клиенты** и просмотрите столбец SSID. Пунктиром отображаются SSID, с которых передаются тестовые сообщения, а клиенты, для которых отображаются SSID, являются связанными клиентами. Нажмите SELECT и выясните, передает ли клиент кадры с тестовыми запросами.

Каковы причины низкой производительности сети или обрыва связи?

- **Достаточен ли уровень мощности сигнала?**

  Выберите **Точки доступа**. На экране **Точки доступа** отображается уровень сигнала для каждой из точек доступа. Выберите точку доступа, чтобы просмотреть дополнительные сведения об уровне сигнала и перегрузке.

- **Сеть слишком занята?**

  Выберите **Каналы** чтобы просмотреть сводку по использованию каналов и количество точек доступа, использующих каждый из каналов. Для отображения диаграммы выделите канал и нажмите SELECT.

- **Есть ли в канале помехи, отличные от помех 802.11?**

  Выберите **Каналы**. Помехи, источником которых не является 802.11, отображаются серым. Этот шум может нарушать подключение в беспроводной локальной сети или снижать скорость сети. Источником постороннего (не 802.11) шума являются микроволновые печи, беспроводные телефоны, устройства Bluetooth®, датчики движения, беспроводные видеокамеры и другие беспроводные устройства.

  Примечание

  Результаты предыдущих трех измерений также отображаются в виде сводки функцией ***Автотест****.*

Существуют ли в сети угрозы безопасности?

- **Поддерживают ли сети предполагаемый уровень безопасности?**

  Выберите **Сети**. Сети, содержащие незащищенные точки доступа, отображаются со значками в виде замков красного цвета ( ).

- **Есть ли в данной области сети с прямым подключением устройств "ad hoc"?**

  Выберите **Сети**. Станции, работающие в режиме "ad hoc", отмечены значком "ad hoc" ( ) в столбце SSID. Станции, работающие в режиме "ad hoc", могут нести угрозу для безопасности сети или могут нарушать политику сети.

  Автотест содержит тест сетей "ad hoc", который выявляет станции, работающие в режиме "ad hoc".

- **Присутствуют ли в данной зоне несанкционированные точки доступа? Где они находятся?**

  AirCheck можно использовать для упрощения отслеживания состояния авторизации обнаруженных точек доступа. По умолчанию при обнаружении точек доступа им присваивается состояние авторизации ? **Неизвестно**. Можно изменить состояние отдельных точек доступа или их групп, чтобы указать на их отношение к данной сети, например, "авторизованная", "соседняя", "неавторизованная".

Также имеется возможность изменить состояние устройств по умолчанию с ? **Неизвестно** на ✓ **Авторизованное**. После изменения все обнаруженные точки доступа будут опознаваться как ✓ **Авторизованное**. Затем можно просмотреть список и назначить надлежащее состояние отдельным точкам доступа. Например, если известно, что точка доступа является несанкционированной, ей можно присвоить состояние **Отмеченное устройство** или ⚠ **Неавторизованное устройство**.

Для задания состояние авторизации устройства по умолчанию выберите **Инструменты > Установить авторизацию устройств по умолчанию (ACL)**.

Для присвоения состояния авторизации точке доступа или группе точек доступа, выберите **Точки доступа**, выделите точку доступа и нажмите F2 **ACL**.

Можно всем точкам доступа присвоить состояние авторизации ✓ **Авторизованное**, выбрав ✓ **Назначить все точки доступа авторизованными**. В результате все обнаруженные точки доступа будут помечены как ✓ **Авторизованное**. При использовании такого подхода, если затем изменить состояние авторизации по умолчанию на ? **Неизвестно**, новые обнаруживаемые точки доступа будут отображаться как ? **Неизвестно**. В целом этот метод обеспечивает быстрое отображение угроз безопасности или новых точек доступа.

Можно также назначить серии точек доступа авторизованными или неавторизованными по BSSID/MAC точки доступа или префиксу MAC поставщика, выбрав **Установить серии ТД в сост. "Автор."** или **Установить серии ТД в сост. "Неавтор."** Эти варианты помогут сберечь время при настройке и оперативно обеспечить отображение потенциальных проблем. Например, если использование оборудования определенного поставщика запрещено политикой сети, используйте префикс MAC данного поставщика для задания данного ACL как неавторизованного. При обнаружении таких точек доступа они автоматически будут отображаться как неавторизованные.

Примечание

При сохранении профиля заданные ACL также сохраняются как часть профиля.

По желанию в "Автотест" можно включить тест на несанкционированные точки доступа, который выявляет несанкционированные точки доступа и уведомляет о них. Для включения этой возможности перейдите на страницу **Инструменты > Пороговые значения/Настройки автотеста > Автотест для несанкционированных точек доступа**.
Для получения точных и поддающихся интерпретации результатов теста перед запуском "Автотеста" требуется настроить ACL точек доступа.

Как можно определить местоположение точки доступа?

Выберите **Точки доступа**, выберите одну точку доступа, затем нажмите F2 **Определить местоположение** на экране **Сведения о точках доступа**. Можно также воспользоваться дополнительной внешней направленной антенной Fluke Networks, которая ускорит поиск точек доступа.

Как составить документ с результатами тестового сеанса и проверки сети?

Сохраните данные сеанса (нажмите 💾), затем используйте программное обеспечение менеджера AirCheck, чтобы загрузить данные на ПК, и создайте отчет.

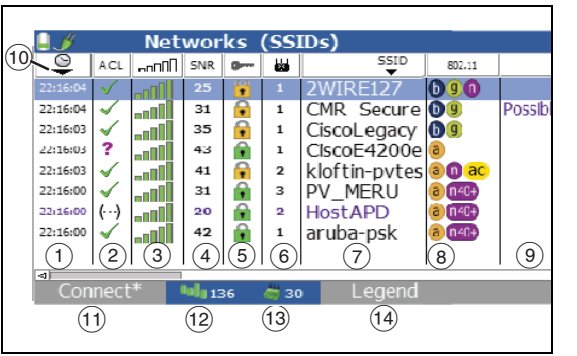
Как удалить всю информацию из AirCheck?

Если требуется удалить из тестера все настройки, данные сеансов и профили, выберите **Инструменты > Удалить все** — удаляются все данные, которые были сохранены и находились в тестере AirCheck.

Обнаружение каналов, сетей, точек доступа или клиентов

Для обнаружения каналов, сетей, точек доступа или клиентов на главном экране выберите **Каналы, Сети, Точки доступа**, или **Клиенты**. На рисунке 2 изображен список **Сети**.

Чтобы просмотреть сведения о сети или точке доступа, с помощью кнопок выделите сети или точки доступа, затем нажмите SELECT.



gdp03a.eps

Рис. 2. Список сетей

① . Время первого обнаружения сети тестером. Для просмотра сетей, которые попадают в зону обнаружения по мере перемещения по участку упорядочите столбец времени списка по убыванию.

Нажмите , затем перемещайтесь по участку. Сети, попадающие в диапазон обнаружения, добавляются в верхнюю часть списка. Сети, выходящие за пределы диапазона обнаружения, если выбран пункт **Отображать необнаруживаемые точки доступа серыми**, будут отображаться серым цветом.

② **ACL**. Состояние авторизации точки доступа. По умолчанию установлено состояние ? **Неизвестно**, но его можно изменить на ✓ **Авторизованное**. Измените состояние каждой из точек доступа, чтобы показать ее отношение к данной сети. Для изменения состояния на главном экране выберите **Точки доступа**, выберите точку доступа и нажмите F2 **ACL**.

(...) – не все точки доступа в сети имеют одинаковое состояние авторизации.

③ ▁▃▅▇ – максимальный уровень мощности сигнала во всех точках доступа для сети с данным SSID.

④ **SNR**. Отношение сигнал/шум измеряет уровень сигнала относительно уровня шума. Это отношение измеряется в децибелах (дБ).

⑤ – состояние безопасности сети:

Красный открытый замок — функция безопасности в сетях не включена.

Примечание

Некоторые сети, отмеченные символами незапертого замка, позволяют подключить тестер и выполнить измерения, в том числе посылку тестовых пакетов Ping, но могут не позволить подключать компьютеры к той же сети для соединения с Интернетом без предъявления идентификатора пользователя и пароля.

Желтый незакрытый замок — одна или несколько точек доступа используют протокол безопасности WEP или Cisco LEAP. Эти протоколы менее безопасны по сравнению с другими протоколами.

Зеленый закрытый замок — во всех точках доступа используются более надежные протоколы безопасности чем протокол WEP, например, WPA или WPA2.

(...) — не все точки доступа используют одинаковый тип безопасности. Например, часть использует WEP, а другая часть использует WPA.

⑥ — число точек доступа, обнаруживаемых тестером в данном местоположении.

⑦ **SSID** — назначенный службой идентификатор. Имя беспроводной сети.

— сеть содержит устройства "ad hoc". Это устройства, которые напрямую, а не через точки доступа, обмениваются данными с другими устройствами. Устройства "ad hoc" могут позволить хакерам получить доступ к данным, передаваемым в сети. (В некоторых политиках для информационной инфраструктуры допускаются устройства "ad hoc".)

[Скрытый] – сеть не передает свой SSID.

⑧ **802.11** – стандарты 802.11, используемые точками доступа в сети:

802.11a – используется в полосе частот 5 ГГц.

802.11b – используется в полосе частот 2,4 ГГц.

802.11g – используется в полосе частот 2,4 ГГц.

802.11n – используется диапазон 2,4 ГГц или 5 ГГц.

802.11ac – используется диапазон 5 ГГц.

Полоски красного цвета — тестер принимает код страны, отличающийся от кода, заданного через меню **Инструменты > Установить страну**. Для идентификации сети или точки доступа, которая передает этот код, выберите **Сети** или **Точки доступа**, затем найдите красные полоски в столбце **802.11**.

n40+ n40– —одна или несколько точек доступа используют объединенный канал. Точки доступа, использующие стандарт 802.11n, могут объединять канал с соседним каналом с более высокой (n40+) или более низкой (n40–) частотой для формирования канала 40 МГц. Такой расширенный канал обеспечивает более высокую пропускную способность сети.

(...) — не во всех точках доступа в сети используется одинаковый стандарт 802.11.

⑨ **Примечания**. Нажмите ▷ для перехода к полю примечаний. Тестер добавляет примечания автоматически. Сети, снабженные примечаниями, отображаются пурпурным цветом.

(...) —сеть снабжена несколькими примечаниями. Для просмотра всех примечаний выделите эту сеть и дважды нажмите SELECT для перехода на экран **Сведения о точке доступа**.

⑩ ▼▲ — **Сортировка 1**, убывающая и возрастающая последовательности.

▼ ▲ — **Сортировка 2**, убывающая и возрастающая последовательности.

Для сортировки списка в возрастающем или убывающем порядке воспользуйтесь ▲ и ◁ ▷ для выделения заголовка столбца, а затем нажмите SELECT или F1 **Сортировка 1**. Например, чтобы быстро найти точку доступа с самым сильным сигналом, выделите ▁▃▅▇ в верхней части столбца, затем нажмите SELECT или F1 **Сортировка 1**. После этого точка доступа с самым сильным сигналом будет отображаться в начале списка.

Для сортировки второго порядка выделите заголовок другого столбца, затем нажмите F2 **Сортировка 2**.

⑪ Нажмите F1 **Подключить** для подключения к выбранной сети.

Кнопка подключения отображается как **Подключить*** (со звездочкой), если тестер не может подключиться к выделенной сети. Для настройки параметров безопасности сети нажмите F1 **Подключить***.

Примечание

Для подключения к защищенной сети тестер должен содержать профиль с регистрационными данными безопасности. Создайте или измените регистрационные данные безопасности в самом тестере или с помощью AirCheck Manager. При нажатии на тестере кнопки ***Подключить**** *запускается процедура настройки конфигурации безопасности. Можно также нажать* ***Инструменты****, затем нажать* ***Управление профилями / паролями сети*** *для изменения настроек безопасности. Звездочка * справа в слове* ***Подключить*** *указывает на то, что настройки безопасности не заданы. Процедуры настройки безопасности с использованием кнопки "Подключить" см. в Руководстве пользователя.*

⑫ — канал, который в данный момент отслеживается тестером. Цвет полосок показывает состояние кода страны по отношению к регулирующему домену.

⑬ — количество точек доступа, которые тестер определяет в данном местоположении. Это количество не учитывает виртуальные точки доступа, если выбран пункт **Группировать виртуальные точки доступа**.

⑭ Для просмотра описания значков на экране **Сети**, нажмите F2 **Легенда**.

Для просмотра подробных данных о точках доступа в сети используйте ▲ ▼ для выделения конкретной сети, а затем нажмите SELECT.

FLUKE networks

AirCheck™
Probador de WiFi

Guía de funcionamiento básico

PN 3434814 12/2009 Rev. 4, 8/13 (Spanish)
©2009-2013 Fluke Corporation. Printed in USA.
All product names are trademarks of their respective companies.
Wi-Fi® is a registered trademark of the Wi-Fi Alliance.

GARANTÍA LIMITADA
Y LIMITACIÓN DE RESPONSABILIDAD

Fluke Networks garantiza que este producto está libre de defectos materiales y mano de obra durante un año a partir de la fecha de compra. Los servicios de reparación de piezas y accesorios están garantizados por 90 días, a menos que se indique lo contrario. Las baterías NiCad, Ni-MH y de iones de litio, los cables y demás periféricos se consideran como piezas o accesorios.

Esta garantía no cubre daños por accidente, negligencia, uso indebido, modificación, contaminación o condiciones anómalas de funcionamiento o manipulación. Los distribuidores no están autorizados para ampliar cualquier otra garantía en nombre de Fluke Networks.

Para solicitar reparaciones durante el período de garantía, comuníquese con el centro autorizado de servicio de Fluke Networks más cercano, quienes le darán información acerca de las autorizaciones de devolución de productos. Después, envíe el producto para su reparación al centro de servicio, junto con una descripción del problema.

ESTA GARANTÍA ES SU ÚNICO RECURSO. NO EXISTE NINGUNA OTRA GARANTÍA, EXPRESA O IMPLÍCITA, COMO LAS DE IDONEIDAD PARA UN FIN ESPECÍFICO Y OTRAS. FLUKE NETWORKS NO SE HACE RESPONSABLE DE NINGÚN DAÑO ESPECIAL, INDIRECTO, PARTICULAR, NI DERIVADO QUE SE PUEDA ALEGAR CON BASE EN CAUSA O TEORÍA ALGUNA.

Dado que algunos estados o países no permiten la exclusión o limitación de las garantías implícitas de daños incidentales o derivados, es posible que este límite de responsabilidad no se aplique a usted.

4/04

Fluke Networks
PO Box 777
Everett, WA 98206-0777
USA

Índice

Acceso al Manual del usuario 1
Información de advertencia 2
Especificaciones generales 5
Mantenimiento, Servicio y Deterioro de protección del equipamiento 5
Comuníquese con Fluke Networks 6
Recarga y vida de las baterías 7
Pantalla de inicio 8
Configuración mínima para un óptimo desempeño 11
¿Qué puede aprender acerca de su red inalámbrica? 12
¿Cuál es la condición de mi red? 12
¿Qué hay en la red inalámbrica? 15
¿Se pueden conectar los dispositivos a la red inalámbrica? 17
¿Qué causa las bajas velocidades de la red y las conexiones desconectadas? 18
¿Existen riesgos de seguridad en la red? 19
¿Cómo puedo localizar un punto de acceso? 22
¿Cómo puedo llevar un registro documentado de mi red y de mi sesión de comprobación? 22
¿Cómo puedo borrar todo en mi AirCheck? 22
Descubrir canales, redes, PA o clientes 23

Acceso al Manual del usuario

Esta guía proporciona información básica para ayudarle a empezar a utilizar el comprobador Wi-Fi AirCheck™. Para obtener más información, consulte el manual del usuario en el CD del producto.

El CD contiene también la aplicación AirCheck Manager, que le ayuda a sacar el máximo partido de su probador.

Información de advertencia

El comprobador Wi-Fi AirCheck ™ es una herramienta portátil especializada para verificar rápidamente y resolver problemas de redes Wi-Fi.

⚠Advertencia⚠

Lea toda la información de seguridad antes de utilizar el producto.

Utilice el producto sólo como se especifica, o la protección proporcionada por el producto puede verse comprometida.

Lea cuidadosamente todas las instrucciones.

Utilice sólo los adaptadores de alimentación aprobados por Fluke para cargar la batería.

No haga funcionar el producto cerca de gas o vapor explosivo o en ambientes húmedos o mojados.

Examine el caso antes de utilizar el producto. Busque las grietas o el plástico que falta. Observe cuidadosamente el material aislante alrededor de los terminales.

Las baterías contienen químicos peligrosos que pueden causar quemaduras o explotar. Si se produce la exposición a productos químicos, limpie con agua y busque ayuda médica.

Quite las baterías si no se ha usado el producto durante un largo período, o si se almacena a temperaturas superiores a 50 °C. Si las baterías no se quitan, el escurrimiento de la batería puede dañar el producto.

No corte los termianles de la batería juntos.

No desarme o aplaste las celdas de la batería.

No ponga las celdas de la batería y las baterías de cerca de fuentes de calor o fuego. No las exponga a la luz solar.

No cargue continuamente las baterías si no las utiliza.

No exponga la batería a impacto mecánico.

No abra la batería. No hay piezas que el usuario pueda reparar en el interior.

Consulte el manual del producto para obtener instrucciones adecuadas sobre la carga de la batería

A fin de evitar posibles incendios, descargas eléctricas, lesiones personales, daños al equipo y resultados inexactos de las pruebas, lea la información de seguridad en el *Manual del usuario del AirCheck* antes de utilizar el comprobador.

	Advertencia y precauciones: riesgo de daño o destrucción del equipo o del software. Consulte las explicaciones en el manual.
	Advertencia: riesgo de descargas eléctricas.
	No deseche productos que contengan tableros de circuito en contenedores de residuos. Consulte las normativas locales para los procedimientos de desecho.
	Este equipo contiene una radio Clase 2.
	Satisface las directivas relevantes de la Unión Europea.
	Cumple con las reglas de la FCC, partes 15.107 y 15.109.
	Listado por la Asociación Canadiense de Normas.

	Satisface los estándares de Australia
	Cumple con los estándares EMC surcoreanos relevantes.

Información adicional sobre los estándares EMC

A급 기기 **(업무용 방송통신기자재)**	이 기기는 업무용 **(A급)** 전자파 적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는 것을 목적으로 합니다.
Equipo de clase A (equipo industrial de transmisión y comunicaciones)	Este es un equipo industrial de ondas electromagnéticas (clase A) y el vendedor o el usuario deben estar al tanto de esto. Este equipo no debe utilizarse en el hogar.

Especificaciones generales

Tipo de batería: Removible y recargable de ión-litio (18,5 vatios-h)

Temperatura de funcionamiento y humedad relativa: 32 °F a 113 °F (0 °C a +45 °C)

Humedad relativa de funcionamiento: (% HR sin condensación) 90 % (50 °F a 95 °F; 10 °C a 35 °C)
75 % (95 °F a 113 °F; 35 °C a 45 °C)

Almacenamiento:-4 °F a 140 °F (-20 °C a +60 °C)

Choques y vibraciones: Aleatorio, 2 g, 5 Hz-500 Hz (Clase 2) prueba de caída de 1 m

Altitud: 4000 m; Almacenamiento: 12000 m

Seguridad: IEC/EN 61010-1

Mantenimiento, Servicio y Deterioro de protección del equipamiento

- La batería es el único componente que el usuario puede reparar. Evite abrir la carcasa; ábrala solamente para reemplazar la batería.
- Utilice únicamente partes de repuesto que estén aprobadas por Fluke Networks.
- Si este equipo se utiliza de alguna forma contraria a lo especificado por el fabricante, la protección que proporciona el equipo podría verse afectada.
- Para limpiar la carcasa, utilice un paño suave humedecido en agua o en agua con un detergente suave.

Comuníquese con Fluke Networks

www.flukenetworks.com
support@flukenetworks.com
+1-425-446-4519

- Australia: 61 (2) 8850-3333 o 61 (3) 9329 0244
- China: 86 (10) 6512-3435
- Brasil: 11 3759 7600
- Canadá: 1-800-363-5853
- Europa: +31-(0) 40 2675 600
- Hong Kong: 852 2721-3228
- Japón: 03-6714-3117
- Corea: 82 2 539-6311
- Singapur: +65-6799-5566
- Taiwán: (886) 2-227-83199
- EE. UU.: 1-800-283-5853

Visite nuestro sitio web para obtener una lista completa de nuestros números telefónicos.

Recarga y vida de las baterías

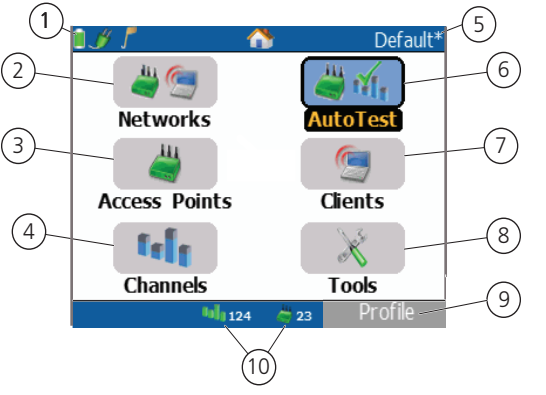
Cargue la batería durante 4 horas antes de utilizarla por primera vez. Para cargar la batería, conecte el adaptador de CA en el conector de la batería en el comprobador de AirCheck.

La batería tiene una duración de unas 5,5 horas en condiciones comunes de uso.

Muestra el estado de la batería. Cuando la carga de la batería es baja, el icono parpadea.

Indica que el adaptador de CA está conectado.

Pantalla de inicio



Inicio.eps

Figura 1. Componentes de la pantalla Home

1

Muestra el estado de la batería. Cuando la carga de la batería es baja, el icono parpadea. Conecte el adaptador de CA para cargar la batería y asegúrese de que el probador siga funcionando.

Indica que el adaptador de CA está conectado.

Indica que la antena externa está conectada.

Nota

AirCheck no transmite ni se conecta a un punto de acceso cuando la antena externa está conectada.

② **Redes**: Descubre redes LAN inalámbricas.

③ **Puntos de acceso**: Descubre puntos de acceso.

④ **Canales**: Indica el uso de canales WLAN.

⑤ El nombre del perfil que el comprobador está utilizando actualmente. El perfil es **Predeterminado** si no se ha cargado un perfil distinto. El campo de nombre contiene un asterisco si se ha cambiado un ajuste en el comprobador desde que se cargó o se guardó el perfil.

⑥ **Autocomprobación**: Comprueba automáticamente el estado de la red verificando la calidad del aire (uso de canales e interferencias), la calidad de red (cobertura de red y conectividad), y la presencia de redes ad hoc. La detección de puntos de acceso indebidos es opcional y exige la configuración de ACL.

⑦ **Clientes**: Descubre clientes que estén utilizando las redes.

⑧ **Herramientas**: Le permite gestionar archivos y configuraciones.

⑨ **Perfil**: Muestra una lista de perfiles disponibles.

⑩ Izquierda: El canal siendo supervisado por el comprobador. El color de las barras indica el estado del código de país del dominio regulatorio. Un ícono rojo puede indicar el funcionamiento de un canal ilegal en la configuración de país actual o la recepción de un código de país diferente.

Derecha: El número de puntos de acceso físico detectados por el comprobador

Es posible almacenar hasta 500 puntos de acceso en la base de datos de puntos de acceso en el comprobador. Cuando el ícono de punto de acceso se pone de color amarillo, indica que se han descubierto 400 o más puntos de acceso.

Cuando el ícono se pone de color rojo, indica que se han descubierto 500 o más puntos de acceso y que la base de datos de punto de acceso está llena. No se incluirán más puntos de acceso descubiertos nuevos en la lista.

Configuración mínima para un óptimo desempeño

Para cambiar el idioma y la configuración de país

1 Seleccione **Herramientas**.

2 Para cambiar el idioma de las pantallas, seleccione **Definir idioma**. Resalte un idioma y, a continuación, presione F2 **Guardar**.

3 Para cambiar el país, seleccione **Definir país**, seleccione el país en el que utilizará el comprobador y presione F2 **Guardar**.

Para obtener el mejor rendimiento de su comprobador, utilice el software AirCheck™ Manager para configurar un perfil y cargarlo en el comprobador. También es posible configurar un perfil en el comprobador de AirCheck. Los perfiles contienen datos que permiten al comprobador realizar las siguientes tareas:

- Conectarse a redes que requieren de credenciales de seguridad.
- Mostrar el estado de autorización correcto para cada punto de acceso. Esto le permite ver rápidamente cuáles puntos de acceso son partes autorizadas de la red.
- Hacer ping a dispositivos claves de la red.
- Ejecutar una prueba de conexión a un puerto TCP utilizando un nombre de host o una dirección IP y un número de puerto designado.

¿Qué puede aprender acerca de su red inalámbrica?

¿Cuál es la condición de mi red?

- **¿Cuál es la calidad de aire de mi conexión Wi-Fi?**
  ¿Están sobrecargados mis canales con puntos de acceso y tráfico Wi-Fi?
  ¿Es alguno de mis canales demasiado ruidoso?

  Seleccione **Autocomprobación**. Después de que la autocomprobación se ha ejecutado, seleccione **Calidad de aire** para ver los resultados de Utilización de canal 802.11, Utilización de canal no 802-11 y Evaluación de estado de interferencia de canales adyacentes.

  En los resultados de Utilización de canal 802.11 se incluye los tres canales que registran el mayor tráfico de Wi-Fi. Se muestra el valor de utilización junto con la calificación de ✓ Aprobado, ⚠ Advertencia o ✗ Reprobado. La nota de la prueba se basa en una comparación entre el valor real y los umbrales configurables por el usuario. Estos umbrales están configurados en **Herramientas > Umbrales / Configuración de autocomprobación**.

  En los resultados de Utilización de canal no 802-11 se incluye los tres canales que registran el mayor grado de interferencia y ruido no 802-11. Se muestra el valor de utilización junto con la calificación de ✓ Aprobado, ⚠ Advertencia o ✗ Reprobado.

En los resultados de Interferencia de canales adyacentes se incluye los tres canales con el mayor AP con un mínimo nivel de potencia y calidad de la señal. Se muestra el recuento de AP además de la calificación de o superior a ✓ Aprobado, ⚠ Advertencia o ✗ Reprobado.

- **¿Cuál es el nivel de calidad de mi red Wi-Fi?**
  ¿Puedo detectar puntos de acceso compatibles con mis redes?
  ¿Hay vacíos de cobertura en esta zona?
  ¿Hay muchos PA cercanos utilizando el mismo canal que estén causando que mi red sea más lenta?
  ¿Puedo conectarme?

  Seleccione **Autocomprobación** - Después de ejecutar la autocomprobación, seleccione **Calidad de Red** para ver los resultados de Cobertura, Interferencia de canales adyacentes, Seguridad y Evaluación de la condición de la conexión.

  En los resultados de Cobertura se incluye el número de PA con buena calidad de señal, incluidos los PA con buena potencia de la señal y los con una buena relación señal/ruido compatibles con una red (SSID), además de la calificación de ✓ Aprobado, ⚠ Advertencia o ✗ Reprobado. El recuento de PA y los umbrales de calidad de señal relativos al nivel de señal y la relación señal/ruido se configuran en las pantallas **Herramientas > Configuración de umbrales / autocomprobación > Cobertura de PA y nivel de señal** y **Umbral señal/ruido**.

En los resultados de Interferencia de canales adyacentes se incluye el número de PA superpuestos en una red además de una calificación de ✓ Aprobado, ⚠ Advertencia o ✗ Reprobado, basado en una comparación de red única respecto a los umbrales. Los umbrales para esta prueba se configuran en la pantalla **Herramientas > Configuración de umbrales / autocomprobación > Umbrales de canales adyacentes de calidad de red**.

En los resultados de Seguridad se indica si todos los PA en el SSID utilizan las mismas las credenciales de seguridad además de una calificación de ✓ Aprobado, ⚠ Advertencia o ✗ Reprobado.

La prueba de conexión intenta conectarse a cada red configurada en su perfil. En los resultados de la prueba de conexión se indica si es posible conectarse a las redes en su ubicación o no con una nota de prueba de Aprobado o Reprobado. Se entregan detalles adicionales acerca de la conexión como el canal, la dirección IP recibida y la velocidad de conexión como una calificación de ✓ Aprobado, ⚠ Advertencia o ✗ Reprobado.

- **¿Qué puntos de acceso no autorizados o desconocidos están conectados a mi red Wi-Fi?**
  ¿Son un riesgo de seguridad?

  La prueba de puntos de acceso indebidos es una parte optativa de la Autocomprobación, indica si se han detectado puntos de acceso desconocidos o no autorizados y realiza una calificación de ✓ Aprobado, ⚠ Advertencia o ✗ Reprobado. En los resultados se incluye una lista de todos los puntos de acceso indebidos detectados en su ubicación. La identificación de los puntos de acceso indebidos requiere la configuración de una Lista de control de acceso (ACL). La configuración de ACL está disponible desde la pantalla de Autocomprobación seleccionando **Puntos de acceso indebidos > ACL** o **Inicio> Puntos de acceso > ACL**.

¿Qué hay en la red inalámbrica?

- **¿Qué redes inalámbricas están disponibles?**

  Seleccione **Redes** para ver una lista de redes LAN inalámbricas y los puntos de acceso que se conectan a cada red. Para ver todos los puntos de acceso que están disponibles en su ubicación, seleccione **Puntos de acceso**.

- **¿Qué puntos de acceso hay disponibles?**
  ¿Son adecuadas las intensidades de la señal?

  Seleccione **Puntos de acceso** para ver una lista de puntos de acceso disponibles en su ubicación y la intensidad de la señal de los puntos de acceso. Para ver los gráficos de barra de intensidad de la señal y el ruido de un punto de acceso, resalte el punto de acceso y, a continuación, presione (SELECT).

- ❑ **¿Está configurado correctamente el punto de acceso?**

  En la pantalla de inicio, seleccione **Puntos de acceso**, resalte un punto de acceso y, a continuación, presione (SELECT).

- ❑ **¿Existen puntos de acceso nuevos en el área? ¿Son sus puntos de acceso, de los vecinos, o un intruso?**

  Utilice la función de estado de autorización del dispositivo (ACL) para informar automáticamente cuando se descubran puntos de acceso nuevos en su ubicación. Para usar esta función, configure el estado de autorización del punto de acceso para cada punto de acceso (por ejemplo, autorizado o vecino), luego establezca el estado de autorización predeterminado en ? **Desconocido**. Como resultado, el estado de autorización predeterminado ? **Desconocido** se asignará a cualquiera punto de acceso que no se haya detectado anteriormente. Por último, seleccione **Puntos de acceso** en la pantalla de inicio para ver los puntos de acceso marcados como ? **Desconocido**.

  Como alternativa, puede guardar la sesión de prueba que incluye la lista de los puntos de acceso detectados. Utilice AirCheck Manager para comparar la lista de puntos de acceso con un archivo de la sesión anteriormente guardada para ver si se detectaron puntos de acceso adicionales.

  Para especificar una autorización de un dispositivo predeterminado desconocido o autorizado, seleccione **Herramientas > Configurar autorización de dispositivo (ACL) predeterminada**

- ❑ **¿Qué clientes inalámbricos usan la red?**

  En la pantalla de inicio, seleccione **Clientes**. También puede desglosar el PA o los detalles del canal para ver la lista de clientes asociados.

¿Se pueden conectar los dispositivos a la red inalámbrica?

Utilice el instrumento para comprobar la conectividad.

- ❑ **¿Puede un dispositivo conectarse a la red (SSID) como un cliente?**

  Seleccione **Redes**, resalte una red y luego presione F1 **Conectar**.

  Nota

  Para conectarse a una red segura, el comprobador debe tener un perfil que incluya las credenciales de seguridad.

- ❑ **¿Puede un dispositivo conectarse a un punto de acceso (BSSID)?**

  Seleccione **Puntos de acceso**, resalte un punto de acceso y, a continuación, presione F1 **Conectar**. Si hay un ***** a la derecha de **Conectar**, esto indica que no se ha configurado la seguridad en el probador para esa red. Presione **Conectar *** y será guiado para ingresar los ajustes de seguridad. Cuando haya terminado, se guarda en el perfil actual. Presione **Herramientas**, luego **Administrar perfiles/contraseñas de red** para volver a editar la configuración de seguridad si es necesario.

- ❑ **Si un dispositivo no se puede conectar a una red o a un punto de acceso, ¿en qué punto ocurre la falla en la conexión?**

  Revise el registro de conexiones. Presione **Registro** F2 en la pantalla **Conectarse a la red** o **Conectarse a punto de acceso**.

- ❑ **¿Puede un dispositivo hacer ping a un dispositivo de la red?**

  Realice una prueba de ping. Conéctese a una red o un punto de acceso y, a continuación, presione F1 **Comenzar pruebas**.

  Nota

  *Los destinos del ping pueden agregarse seleccionando **Herramientas > Administrar perfiles/contraseñas de red > Editar destinos > Agregar**. Puede agregar un destino con una dirección IP o el nombre de host (URL).*

  *Si hay un ***** a la derecha de **Conectar**, esto indica que no se ha configurado la seguridad en el probador para esa red. Presione **Conectar *** y será guiado para ingresar los ajustes de seguridad.*

- ❑ **¿Funciona correctamente la tarjeta de red de un cliente?**

  Seleccione **Clientes** y, a continuación, busque en la columna de SSID. Los SSID con rayas sondean los clientes y los clientes con un nombre de SSID son los clientes asociados. Presione SELECT y vea si el cliente transmite tramas de solicitud de sonda.

¿Qué causa las bajas velocidades de la red y las conexiones desconectadas?

- ❑ **¿Tiene la señal la intensidad suficiente?**

  Seleccione **Puntos de acceso**. La pantalla **Puntos de acceso** muestra la intensidad de la señal para cada punto de acceso. Seleccione un punto de acceso para ver más información sobre la intensidad de la señal y la congestión.

- **¿Está congestionada la red?**

  Seleccione **Canales** para ver una descripción general del uso del canal y el número de puntos de acceso que usan cada canal. Para ver un gráfico, resalte un canal y, a continuación, presione SELECT.

- **¿Hay interferencia de señales distintas de las 802.11 en un canal dado?**

  Seleccione **Canales**. La interferencia que no es 802.11 es gris. Este ruido puede interferir con las conexiones WLAN o el rendimiento. El ruido que no es 802.11 puede provenir de hornos microondas, teléfonos inalámbricos, dispositivos Bluetooth®, detectores de movimiento, cámaras inalámbricas y otros dispositivos inalámbricos.

  Nota

  *Las tres mediciones anteriores se resumen también en la función **Autocomprobación**.*

¿Existen riesgos de seguridad en la red?

- **¿Tienen las redes el nivel esperado de seguridad?**

  Seleccione **Redes**. Las redes que tienen puntos de acceso no seguros aparecen con un candado rojo ( ).

- **¿Existen redes ad hoc en la zona?**

  Seleccione **Redes**. Las estaciones que están funcionando en modo de red ad hoc se marcarán con el icono ad hoc () en la columna de SSID. Las estaciones ad hoc pueden ser riesgos para la seguridad de la red o pueden violar las políticas de red.

Autocomprobación incluye una prueba de Red Ad Hoc que marca las estaciones ad hoc.

- ❑ **¿Existen puntos de acceso intrusos en el área? ¿Dónde están?**

  Se puede usar AirCheck para ayudar a controlar el estado de la autorización de los puntos de acceso detectados. De manera predeterminada, cuando se detectan puntos de acceso, se les asigna un estado de autorización ? **Desconocido**. Puede cambiar el estado de puntos de acceso individuales o en grupo para reflejar su relación con la red, por ejemplo, autorizado, vecino, no autorizado.

  También tiene la opción de modificar el estado del dispositivo predeterminado de ? **Desconocido** a ✓**Autorizado**. Una vez modificado, todos puntos de acceso detectados se identificarán como ✓**Autorizado**. A continuación, puede revisar la lista y asignar un estado a cada uno de los puntos de acceso según corresponda. Por ejemplo, si sabe que un punto de acceso es un intruso, puede asignarle el estado de **Dispositivo marcado** o ⚠**Dispositivo no autorizado**.

  Para especificar una autorización de dispositivo predeterminado, seleccione **Herramientas > Configurar autorización de dispositivo (ACL) predeterminada**.

  Para darle a un punto de acceso o grupo de puntos de acceso un estado de autorización, seleccione **Puntos de acceso**, resalte un punto de acceso y, a continuación, presione F2 **ACL**.

Puede establecer el estado de autorización para todos los puntos de acceso en ✓ **Autorizado** al seleccionar ✓ **Establecer todos los AP en Autorizado**. Esto hará que todos los puntos de acceso detectados se marquen como ✓ **Autorizado**. Con este enfoque, cuando el estado de autorización predeterminada se establezca en ? **Desconocido**, los puntos de acceso de detección reciente aparecerán como ? **Desconocido**. En general, este método proporciona una visibilidad rápida de los riesgos de seguridad o los puntos de acceso nuevos.

También puede establecer una serie de PA como autorizado o no autorizado en función de la BSSID/MAC del PA o un prefijo MAC del proveedor al seleccionar ✓ **Establecer serie de PA en Autorizado** o ⚠ **Establecer serie de PA en No autorizado**. Estas opciones pueden ahorrar tiempo de configuración y proporcionar una visibilidad rápida ante problemas potenciales. Por ejemplo, si el equipo de un proveedor específico no se permite debido a su política de redes, use el prefijo de MAC del proveedor para establecer la ACL en no autorizado. Cuando se detectan esos puntos de acceso, estos se informarán automáticamente considerado como no autorizados.

Nota

Al guardar el perfil, los ACL asignados también se guardan como parte de ese perfil.

Opcionalmente, la Autocomprobación incluye también una Prueba de Punto de acceso intruso que detecta e informa los puntos de acceso intrusos. Para habilitar esta funcionalidad, vaya a **Herramientas > Umbrales/Configuración de autocomprobación > Autocomprobación de punto de acceso intruso**. Para obtener resultados precisos y significativos de la prueba, debe configurar las ACL del punto de acceso antes de ejecutar la autocomprobación.

¿Cómo puedo localizar un punto de acceso?

Seleccione **Puntos de acceso**, seleccione un punto de acceso y, a continuación, presione F2 **Localizar** en la pantalla **Detalles del punto de acceso**. También puede utilizar la antena direccional externa Fluke Networks opcional para ayudarle a encontrar puntos de acceso más rápido.

¿Cómo puedo llevar un registro documentado de mi red y de mi sesión de comprobación?

Guarde la sesión (presione 💾), y luego utilice el software AirCheck Manager para descargar la información a una PC y hacer un informe.

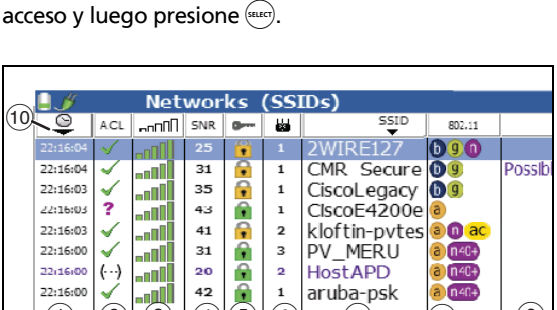
¿Cómo puedo borrar todo en mi AirCheck?

Si desea borrar todas las configuraciones, datos de sesión y los perfiles del probador, seleccione **Herramientas > Borrar todo** - Se borra todo lo que se haya guardado o almacenado en el probador AirCheck.

Descubrir canales, redes, PA o clientes

Para descubrir canales, redes, puntos de acceso o clientes, seleccione **Canales**, **Redes, Puntos de acceso** o **Clientes** en La pantalla de inicio. La figura 2 muestra una lista de **Redes**.

Para ver detalles acerca de una red o de un punto de acceso, utilice ▲ ▼ para resaltar la red o el punto de acceso y luego presione SELECT.



gdp03a.eps

Figura 2. Lista de redes

① : La primera vez que el probador sabe de la red. Para ver las redes que están dentro del alcance a medida que se mueve por el área, ordene la lista en orden descendente para la columna de sello de tiempo.

Presione y, a continuación, muévase por el área. Las redes que entran en el rango se agregan a la parte superior de la lista. Las redes que se encuentren fuera del rango pasarán a ser grises si **Puntos de acceso inaudibles grises** está activado.

② **ACL**: El estado de autorización del punto de acceso. El estado predeterminado es ? **Desconocido**, pero puede cambiarse a ✓ **Autorizado**. Cambie el estado de cada punto de acceso para mostrar cómo se relaciona con la red. Para cambiar el estado, seleccione **Puntos de acceso** en la pantalla de inicio, seleccione un punto de acceso y, a continuación, presione F2 **ACL**.

(...): no todos los puntos de acceso de la red tienen el mismo estado de la autorización.

③ : la máxima intensidad de la señal de los puntos de acceso de una red (SSID).

④ **SNR**: Nivel de señal a ruido es una medida de intensidad de la señal con respecto al ruido. La relación se mide en decibelios (dB).

⑤ : el estado de la seguridad de la red.

Candado rojo abierto: la red no tiene habilitada la seguridad.

Nota

Algunas redes con un candado abierto permiten conectar el probador y realizar mediciones incluida la ejecución de la prueba de Ping, pero no permiten que una PC se conecte a la misma red para conectarse a la web sin un ID de usuario y contraseña.

Candado amarillo cerrado: uno o más puntos de acceso utilizan protocolos de seguridad WEP o Cisco LEAP. Estos son menos seguros que otros protocolos.

Candado verde cerrado: todos los puntos de acceso utilizan protocolos de seguridad más seguros que el WEP, por ejemplo, el WPA o el WPA2.

(...): todos los puntos de acceso en la red no utilizan el mismo tipo de seguridad. Por ejemplo, uno utiliza WEP mientras que otro utiliza WPA.

⑥ : la cantidad de puntos de acceso que detecta el probador en la presente ubicación.

⑦ **SSID**: Siglas de identificador de conjunto de servicios. El nombre de la red inalámbrica.

: la red tiene dispositivos ad hoc. Estos son los dispositivos que se comunican directamente con otros dispositivos, no a través de un punto de acceso. Los dispositivos ad hoc pueden dar a los hackers acceso a datos que se transmiten en la red (algunas políticas de IT para redes permiten dispositivos ad hoc).

[Oculto]: el dispositivo no transmite su identificador SSID.

⑧ **802.11**: indica cuál de las normas 802.1 es la utilizada por el correspondiente punto de acceso:

802.11a: utiliza la banda de 5 GHz.

802.11b: utiliza la banda de 2.4 GHz.

802.11g: utiliza la banda de 2.4 GHz.

802.11n: utiliza la banda de 2.4 GHz o 5 GHz.

802.11ac: utiliza la banda de 5 GHz.

Barras rojas: el probador recibió un código de país que es diferente de la configuración en **Herramientas** > **Configurar país**. Para identificar la red o el punto de acceso que transmite el código, seleccione **Redes** o **Puntos de acceso**, luego busque las barras rojas en la columna **802.11**.

n40+ n40–: uno o más puntos de acceso utilizan un canal vinculado. Los puntos de acceso que utilizan la norma 802.11n pueden unir un canal a un canal de extensión por encima (n40+) o por debajo (n40–) para formar un canal de 40 MHz. Este canal más ancho le da a la red mayor velocidad.

(...): indica que no todos los puntos de acceso de la red utilizan la misma norma 802.11.

⑨ **Notas**: pulse ▷ para desplazarse al campo de notas. El comprobador añade notas automáticamente. Las redes que tienen notas se muestran en color púrpura.

(...): la red tiene diversas notas. Para ver todas las notas, resalte la red, luego presione SELECT dos veces para ir a la pantalla de **Detalles del punto de acceso**.

⑩ ▼▲: **Ordenar 1**, secuencias descendentes y ascendentes.

▼ ▲ : **Ordenar 2**, secuencias descendentes y ascendentes.

Para ordenar la lista en secuencia ascendente o descendente, utilice ▲ y ◀ ▶ para resaltar el encabezado de una columna, luego presione SELECT o F1 **Ordenar 1**. Por ejemplo, para encontrar rápidamente el punto de acceso que tiene la señal más potente, resalte ⎍⎍⎍⎍ en la parte superior de la columna, a continuación, presione SELECT o F1 **Ordenar 1**. Esto coloca al punto de acceso con la señal más potente en la parte superior de la lista.

Para ordenar en una secuencia secundaria, resalte un encabezado de columna distinto y luego presione F2 **Ordenar 2**.

(11) Presione F1 **Conectar** para conectarse a la red resaltada.

El botón de conexión muestra **Conectar*** (con un asterisco) si el probador no puede conectarse a la red resaltada. Para configurar la seguridad de la red, presione F1 **Conectar***.

Nota

Para conectarse a una red segura, el pobrador debe tener un perfil que incluya credenciales de seguridad. Cree o edite las credenciales de seguridad en el probador o con AirCheck Manager. Cuando presione ***Conectar**** *en el probador, este le guiará a través de la configuración de seguridad. También puede presionar* ***Herramientas****, luego* ***Administrar perfiles /contraseñas de red*** *para volver a configurar las opciones de seguridad. El* ***** *a la derecha de* ***Conectar*** *indica que ninguna opción de seguridad se ha configurado. Consulte el Manual del usuario para configurar los procedimientos de seguridad utilizando Conectar.*

⑫

: El probador que actualmente monitorea el canal. El color de las barras indica el estado del código de país para el dominio regulador.

⑬

: La cantidad de puntos de acceso que el probador detecta en su ubicación. La cantidad detectada no incluye los puntos de acceso virtuales si se selecciona **Agrupar puntos de acceso virtuales**.

⑭ Para ver las descripciones de los iconos en la pantalla de **Redes**, presione F2 **Leyenda**.

Para ver información detallada acerca de los puntos de acceso de una red, utilice ▲ ▼ para resaltar una red y luego presione SELECT.

FLUKE networks

AirCheck™
Wi-Fi テスター

スタート・ガイド

PN 3434814 12/2009 Rev. 4, 8/13 (Japanese)
©2009-2013 Fluke Corporation. Printed in USA.
All product names are trademarks of their respective companies.
Wi-Fi® is a registered trademark of the Wi-Fi Alliance.

限定保証および補償責任限度

フルーク･ネットワークスは、本製品に材料および製造上の欠陥がないことを保証します。保証期間はご購入日から 1 年間です。部品、アクセサリー、製品の修理、およびサービスに関する保証期間は、特に明記していない限り 90 日間です。ニッカド、Ni-MH およびリチウムイオン･バッテリー、ケーブル、その他の周辺装置は、部品またはアクセサリーとして扱われます。

この保証は、事故、不注意、誤用、改造、汚染された状況下での使用、もしくは異常な操作や取り扱いによって生じた損傷については適用されません。指定販売業者が、フルーク･ネットワークスに代わって付加的な保証を与える権限はありません。

保証期間中にサービスを受けるには、最寄りのフルーク･ネットワークス認定サービス･センターにご連絡の上、返送に関する承認を得た後、問題点の説明を添えてサービス･センターに製品をご返送ください。

本保証はお客様への唯一の保証内容です。特定の目的に対する適合性など、その他の保証を明示または黙示するものではありません。フルーク･ネットワークスは、いかなる原因または理由においても、本製品の使用から生ずる特例的、間接的、偶発的、または派生的な損害または損失に対する保証の責任を負いません。

一部の国や州においては、暗黙の保証に制限を付けること、あるいは偶発的または必然的な損傷を除外したり限定したりすることを許していないため、本保証における制限および除外は、すべてのお客様に適用されるわけではありません。

4/04

Fluke Networks
PO Box 777
Everett, WA 98206-0777
USA

目次

ユーザーズ･マニュアルの利用 1
警告に関する情報. 2
　一般仕様 5
　保守、サービスおよび機器の安全保護機能の損傷 6
フルーク･ネットワークスの連絡先 7
バッテリーの充電と稼働時間 8
ホーム画面. 9
最高のパフォーマンスを得るための最小要件. . . 12
無線ネットワークについて把握できること 13
　ネットワークの健全性について. 13
　無線 LAN について 16
　デバイスと無線ネットワークの接続可能性について 18
　ネットワーク･パフォーマンスの遅延および接続性が失われる原因について 19
　ネットワークのセキュリティー･リスクについて 20
　アクセス･ポイントの特定方法. 23
　マイ･ネットワークおよびマイ･テスト･セッションの記録方法. 23
　AirCheck のすべての情報を消去する方法. . . . 23
チャネル、ネットワーク、AP、またはクライアントの検出. 24

ユーザーズ･マニュアルの利用

本ガイドには、AirCheck™ Wi-Fi Tester を使い始めるための基本情報が記載されています。詳しい情報については、製品 CD に収録されているユーザーズ･マニュアルを参照してください。

この CD には、テスターを最大限に活用するために役立つ AirCheck マネージャー･アプリケーションも収録されています。

警告に関する情報

AirCheck ™ Wi-Fi Tester は、Wi-Fi ネットワークの検証およびトラブルシューティングを短時間で行うための専用ハンドヘルド･ツールです。

⚠ 警告 ⚠

本器を使用する前に、すべての安全上の注意をお読みください。

本器は指定されたとおりに使用してください。そうでない場合、本器で提供される保護が損なわれる可能性があります。

すべての指示をよくお読みください。

バッテリーを充電するには、フルーク認定の電源アダプターのみを使用してください。

爆発性のガス、蒸気の周り、または水気の多い湿った環境で本器を使用しないでください。

本器を使用する前にケースを確認してください。プラスチックの亀裂や不足がないか確認してください。端子の周りの絶縁を慎重に確認してください。

有害化学物質を含んでいるバッテリーはやけどや爆発が発生する可能性があります。化学物質にさらされた場合は、水で洗浄し医師の診察を受けてください。

本器を長時間使用しない場合、または 50 °C を超える温度で保管する場合は、バッテリーを取り外してください。取り外さないと、バッテリーの液漏れにより本器が損傷する可能性があります。

バッテリー端子を互いに短絡させないでください。

バッテリー・セルまたはバッテリー・パックを分解または粉砕しないでください。

バッテリー・セルやバッテリー・パックを熱や火の近くに置かないでください。また、直射日光にさらさないでください。

使用しないときに、バッテリー・パックを連続充電しないでください。

バッテリー・パックに機械的衝撃を与えないでください。

バッテリー・パックを開放しないでください。ユーザーが修理できる部品は内部にありません。

バッテリー・パックの充電の正しい手順については、製品マニュアルを参照してください。

火災、感電、その他の怪我、本器への損傷、不正確なテスト結果を避けるため、本器を使用する前に、『AirCheck ユーザーズ・マニュアル』の「安全に関する情報」をお読みください。

	警告または注意 : 機器またはソフトウェアの破損または破壊の危険性があります。マニュアルの説明を参照してください。
	警告 : 感電の危険性があります。
	回路基板を含む製品は、一般ごみとして捨てないでください。破棄手順については、地域の法律に従ってください。
	本機器には、クラス 2 の無線が含まれています。
	関連する EU 加盟国基準に準拠しています。
	FCC 規定、パート 15.107、15.109 に準拠しています。
	Canadian Standards Association により承認済みです。
	関連するオーストラリアの規格に準拠しています。
	関連する韓国の EMC 規格に準拠しています。

韓国の EMC 規格に関する追加情報 :

電磁適合性。韓国内での使用のみに適用。クラス A 機器 (放送および通信産業用機器)[1]	[1] 本製品は産業用 (クラス A) 電磁機器の要件に適合しています。販売者またはユーザーはこの点を認識している必要があります。本機器は業務での使用を目的としており、家庭での使用は考慮されていません)

一般仕様

バッテリー・タイプ : 着脱式、充電式リチウムイオン・バッテリー・パック (18.5Wh)

作動温度および相対湿度 : 0°C ～ +45°C

作動相対湿度 : (% RH、結露なし) 90 % (10°C ～ 35°C) 75 % (35°C ～ 45°C)

保管時 : -20°C ～ +60°C

衝撃と振動 : ランダム、2 g、5 Hz ～ 500 Hz (クラス 2)、1 m 落下テスト

高度 : 4,000 m、保管時 : 12,000 m

安全性 : IEC/EN 61010-1

保守、サービスおよび機器の安全保護機能の損傷

- ユーザーが交換可能な部品はバッテリーだけです。バッテリーを交換する以外には、ケースを開けないでください。
- フルーク･ネットワークス指定の交換部品のみを使用してください。
- 本器は、このマニュアルに記載されている方法でのみ使用してください。これを怠ると、本器の安全保護機能が損なわれる可能性があります。
- ケースをクリーニングする際には、水または水と中性洗剤で湿らせた柔らかい布を使用してください。

フルーク･ネットワークスの連絡先

www.flukenetworks.com

support@flukenetworks.com

+1-425-446-4519

- オーストラリア : 61 (2) 8850-3333 または 61 (3) 9329 0244
- 北京 : 86 (10) 6512-3435
- ブラジル : 11 3759 7600
- カナダ : 1-800-363-5853
- ヨーロッパ : +31 -(0) 40 2675 600
- 香港 : 852 2721-3228
- 日本 : 03-6714-3117
- 韓国 : 82 2 539-6311
- シンガポール : +65-6799-5566
- 台湾 : (886) 2-227-83199
- 米国 : 1-800-283-5853

電話番号の全一覧については、フルーク･ネットワークスの Web サイトをご覧ください。

バッテリーの充電と稼働時間

バッテリーを初めて使用する前に、4 時間充電してください。バッテリーを充電するには、AC アダプターを AirCheck テスターのバッテリー･コネクターに接続します。

標準的な使用におけるバッテリーの稼動時間は約 5.5 時間です。

バッテリーの状態を示します。残量が少なくなると、このアイコンが点滅します。

AC アダプターが接続されていることを示します。

ホーム画面

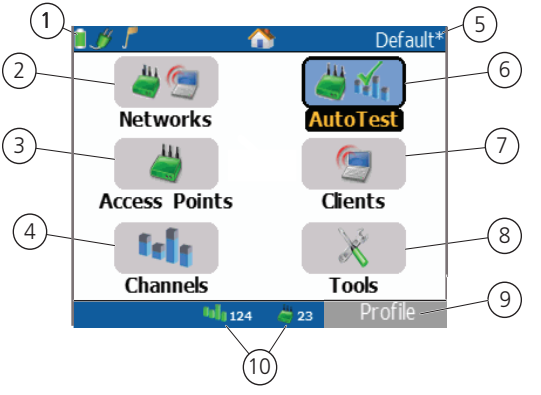


図 1. ホーム画面の構成要素

①

バッテリーの状態を示します。残量が少なくなると、このアイコンが点滅します。AC アダプターを接続してバッテリーを充電し、テスターが作動し続けることを確認してください。

AC アダプターが接続されていることを示します。

外付けアンテナが接続されていることを示します。

注記

外付けアンテナが接続されている場合、AirCheck はアクセス･ポイントに送信または接続しません。

② **[ネットワーク]**: 無線 LAN を検出します。

③ **[アクセス･ポイント]**: アクセス･ポイントを検出します。

④ **[チャネル]**: WLAN チャネルの利用状況を示します。

⑤ テスターが現在使用しているプロファイルの名前。プロファイル名は、別のプロファイルを読み込んでいない場合、**[デフォルト]** と表示されます。プロファイルの読み込みまたは保存後にテスターの設定を変更した場合は、プロファイル名にアスタリスク記号が付きます。

⑥ **[オートテスト]**: 無線品質 (チャネル使用率および干渉)、ネットワーク品質 (ネットワークのカバレッジおよび接続性)、アド･ホック･ネットワークの有無を調べて、ネットワークの健全性を自動的に確認します。不正アクセス･ポイントの検出はオプションであり、これを実行するには ACL を構成する必要があります。

⑦ **[クライアント]**: ネットワークを使用してクライアントを検出します。

⑧ **[ツール]**: ファイルや設定の管理に使用します。

⑨ **[プロファイル]**: 使用可能なプロファイルのリストを表示します。

⑩ 左側: テスターが現在モニターしているチャネル。バーの色は規制領域に対する国コードのステータスを示します。赤のアイコンは、現在の国設定に対して不正チャネルが作動していること、または異なる国コードが受信されていることを示します。

右側: テスターが認識できる物理アクセス･ポイント数。

テスターのアクセス･ポイント･データベースには、最大 500 のアクセス･ポイントを格納できます。アクセス･ポイントのアイコンが黄色になった場合は､400 以上のアクセス･ポイントが検出されています。

このアイコンが赤色になった場合は、500 以上のアクセス･ポイントが検出されていて､アクセス･ポイント･データベースがいっぱいになっています。新たに検出されたアクセス･ポイントは、リストに表示されません。

最高のパフォーマンスを得るための最小要件

言語と国の設定の変更方法

1 **[ツール]** を選択します。

2 画面に表示される言語を変更するには、**[言語の設定]** を選択します。言語を反転表示してから F2 **[保存]** を押します。

3 国を変更するには **[国設定]** を選択し、テスターを使用する国を選択してから、F2 **[保存]** を押します。

テスターのパフォーマンスを最適化するには、AirCheck™ Manager ソフトウェアを使用してプロファイルを設定し、テスターにアップロードします。プロファイルは AirCheck テスターで設定することもでき、プロファイルにはテスターが次のタスクを実行するためのデータが含まれます。

- セキュリティー証明書を必要とするネットワークへの接続。
- 各アクセス･ポイントの正確な承認ステータスの表示。これにより、ネットワーク内のどのアクセス･ポイントが承認済みであるかをすばやく確認できます。
- キー･ネットワーク･デバイスへの Ping。
- TCP ポート接続テストの実行。ホスト名または IP アドレス、および指定されたポート番号を使用します。

無線ネットワークについて把握できること

ネットワークの健全性について

- **Wi-Fi 無線品質はどの程度か？**
  使用しているチャネルがアクセス･ポイントおよび Wi-Fi トラフィックによって過負荷になっていないか？
  ノイズが大きくなりすぎているチャネルはないか？

  [オートテスト] を選択します。[オートテスト] を実行したら、**[無線品質]** を選択して、802.11 チャネル使用率、非 802.11 チャネル使用率、およびチャネル間干渉についての健全性評価の結果を表示します。

  802.11 チャネル使用率の結果には、Wi-Fi トラフィックが最大になっている、最もビジーな上位 3 つのチャネルが含まれています。チャネル使用率は、✓ (合格)、⚠ (警告)、または ✗ (不合格) の評価とともに表示されます。テストの評価は、実際の値とユーザーが設定可能なしきい値を比較して判別されます。これらのしきい値は **[ツール] > [Thresholds / AutoTest Settings (しきい値/オートテストの設定)]** で設定できます。

  非 802.11 チャネル使用率の結果には、非 802.11 干渉とノイズが最大の上位 3 つのチャネルが含まれています。チャネル使用率は、✓ (合格)、⚠ (警告)、または ✗ (不合格) の評価とともに表示されます。

  チャネル間干渉の結果には、信号強度と信号品質が最低で、AP 数が最も多い上位 3 つのチャネルが含まれています。AP 数は、✓ (合格)、⚠ (警告)、または ✗ (不合格) の評価とともに表示されます。

❑ **Wi-Fi ネットワーク品質はどの程度か？**
使用しているネットワークをサポートするアクセス･ポイントを認識できるか？
このエリア内に対象範囲外の部分は存在するか？
同じチャネルを使用する近接 AP が多すぎて、ネットワーク速度が低下していないか？
接続できるか？

[オートテスト] を選択します。[オートテスト] が実行されたら、**[ネットワーク品質]** を選択して、カバレッジ、チャネル間干渉、セキュリティー、および接続に関する健全性評価を表示します。

カバレッジの結果には、信号強度と信号対ノイズ比を含めて信号品質が良好であり、かつネットワーク (SSID) をサポートする AP の数が、(合格)、(警告)、または ⚠ (不合格) の評価とともに表示されます。テストの評価は、実際の値とユーザーが設定可能なしきい値を比較して判別されます。AP 数、および信号レベルと信号対ノイズ比からなる信号品質しきい値は、[ツール] > [Thresholds / AutoTest Settings (しきい値/オートテストの設定)] の順に選択して表示される [AP Coverage (AP カバレッジ)]、[信号レベル]、[Signal-to-noise Threshold (信号対ノイズ比のしきい値)] の各画面で設定します。✓ ✗

チャネル間干渉の結果には、単一ネットワークとしきい値の比較に基づき、ネットワークの重複 AP 数が ✓ (合格)、⚠ (警告)、または ✗ (不合格) の評価とともに表示されます。このテストのしきい値は、**[ツール] > [Thresholds / AutoTest Settings (しきい値/オートテストの設定)] > [Network Quality co-channel thresholds (ネットワーク品質チャネル間しきい値)]** 画面で設定します。

セキュリティーの結果では、SSID のすべての AP で同じセキュリティー証明書が使用されているかどうかが、✓（合格）、⚠（警告）、または ✗（不合格）の評価とともに報告されます。

接続テストでは、プロファイルで設定された各ネットワークに接続しようとします。そのテスト結果として、ご使用の場所からネットワークに接続できるかどうかが、[合格] または [不合格] の評価を使って示されます。チャネル、受信した IP アドレス、接続速度などの接続の詳細情報も、✓（合格）、⚠（警告）、または ✗（不合格）の評価を使って示されます。

- **Wi-Fi ネットワークに未承認または不明のアクセス・ポイントが接続されているか？ これらはセキュリティー・リスクなのか？**

  不正アクセス・ポイント・テストは、オートテストに含まれるオプションのテストです。未承認または不明のアクセス・ポイントが検出されているかどうかが、✓（合格）、⚠（警告）、または ✗（不合格）の評価で示されます。結果には、ご使用の場所で認識されたすべての不正アクセス・ポイントのリストが含まれます。不正アクセス・ポイントを識別するには、アクセス・コントロール・リスト (ACL) を設定する必要があります。ACL の設定は、**[Rogue Access Points (不正アクセス・ポイント)] > [ACL]** または **[ホーム] > [アクセス・ポイント] > [ACL]** を選択して表示される、[オートテスト] 画面で行います。

無線 LAN について

- ❑ **使用可能な無線 LAN は？**

  [ネットワーク] を選択して、各ネットワークに接続されている無線 LAN およびアクセス･ポイントのリストを表示します。ご使用の場所で使用できるアクセス･ポイントをすべて表示するには、**[アクセス･ポイント]** を選択します。

- ❑ **どのアクセス･ポイントを使用できるか？信号強度は十分か？**

  [アクセス･ポイント] を選択して、ご使用の場所で利用可能なアクセス･ポイントと各アクセス･ポイントの信号強度のリストを表示します。アクセス･ポイントの信号強度とノイズを棒グラフで表示するには、アクセス･ポイントを反転表示してから、SELECT を押します。

- ❑ **アクセス･ポイントは正しく設定されているか？**

  ホーム画面で **[アクセス･ポイント]** を選択し、アクセス･ポイントを反転表示してから、SELECT を押します。

- ❑ **エリア内に新しいアクセス･ポイントがあるか？それは使用中のアクセス･ポイントか、近接アクセス･ポイントか、それとも不正アクセス･ポイントか？**

デバイス承認ステータス (ACL) 機能を使用して、ご使用の場所で新しいアクセス･ポイントが検出された場合は自動的に報告されるようにします。この機能を利用するには、各アクセス･ポイントのアクセス･ポイント承認ステータス (承認済みまたは近接など) を設定してから、デフォルトの承認ステータスを **？ (不明)** に設定します。こうすることで、以前は検出されなかったアクセス･ポイントに、デフォルトの承認ステータスである **？ (不明)** が割り当てられます。最後に、ホーム画面で **[アクセス･ポイント]** を選択し、**？ (不明)** とマークされたアクセス･ポイントをすべて表示します。

または、検出されたアクセス･ポイントのリストが含まれているテスト･セッションを保存します。AirCheck マネージャーを使用して、アクセス･ポイントのリストと保存済みのセッション･ファイルを比較して、新たなアクセス･ポイントが検出されているかどうかを確認します。

デフォルトのデバイス承認ステータス (不明、または承認済み) を指定するには、**[ツール] > [Set Device Authorization (ACL) default (デバイス承認 (ACL) のデフォルトを設定)]** を選択します。

- ❑ **ネットワークを使用している無線クライアントを確認できるか？**

  ホーム仮面で、**[クライアント]** を選択します。AP またはチャネルの詳細までドリルダウンして、関連するクライアントのリストを表示することもできます。

デバイスと無線ネットワークの接続可能性について

テスターを使用して接続性を検査します。

- ❑ **デバイスはクライアントとしてネットワーク (SSID) に接続できるか？**

  [ネットワーク] を選択してネットワークを反転表示してから、F1 **[接続]** を押します。

  注記

  安全なネットワークに接続するには、テスターに、セキュリティー証明書を含むプロファイルが必要です。

- ❑ **デバイスはアクセス･ポイント (BSSID) に接続できるか？**

  [アクセス･ポイント] を選択し、アクセス･ポイントを反転表示してから、F1 **[接続]** を押します。**[接続]** の右に * が表示されている場合は、このネットワークのテスターにセキュリティーが設定されていません。**[接続 *]** を押すと、セキュリティー設定の入力方法がガイドされます。設定が完了すると、設定内容が現在のプロファイルに保存されます。**[ツール]** をクリックしてから、**[Manage profiles / network passwords (プロファイル/ネットワーク･パスワードの管理)]** をクリックして、必要に応じてセキュリティー設定を再編集します。

- ❑ **デバイスがネットワークまたはアクセス･ポイントに接続できない場合、どの段階で接続に失敗するのか？**

  接続ログを確認します。**[ネットワークへの接続]** または **[アクセス･ポイントへの接続]** 画面で F2 **[ログ]** を押します。

❑ **デバイスはネットワーク･デバイスに Ping できるか？**

Ping テストを実行します。ネットワークまたはアクセス･ポイントに接続してから、F1 **[テストの開始]** を押します。

注記

Ping ターゲットを追加するには、[ツール] > [Manage profiles / network passwords (プロファイル/ネットワーク･パスワードの管理)] > [Edit targets (ターゲットの編集)] > [追加] を選択します。IP アドレスまたはホスト名 (URL) を使ってターゲットを追加できます。

[接続] の右に * が表示されている場合は、このネットワークのテスターにセキュリティーが設定されていません。[接続 *] を押すと、セキュリティー設定の入力方法がガイドされます。

❑ **クライアントのネットワーク･インタフェース･カードは正しく動作するか？**

[クライアント] を選択して、SSID 列を確認します。SSID が破線の場合は、クライアントをプロービングしています。SSID 名が表示されているクライアントは、関連付けられたクライアントです。SELECT を押して、クライアントがプローブ･リクエスト･フレームを送信しているかどうかを確認します。

ネットワーク･パフォーマンスの遅延および接続性が失われる原因について

❑ **信号強度は十分か？**

[アクセス･ポイント] を選択します。**[アクセス･ポイント]** 画面に、各アクセス･ポイントの信号強度が表示されます。アクセス･ポイントを選択して、信号強度および輻輳の詳細を表示します。

❑ **ネットワークがビジー状態か？**

[チャネル] を選択して、チャネル使用率、および各チャネルを使用するアクセス･ポイント数の概要を確認します。グラフを表示するには、チャネルを反転表示して、SELECT を押します。

❑ **チャネル上に非 802.11 干渉があるか？**

[チャネル] を選択します。非 802.11 干渉はグレーで表示されます。このノイズは WLAN 接続またはパフォーマンスに悪影響を与えることがあります。非 802.11 ノイズは、電子レンジ、コードレス電話、Bluetooth® デバイス、動作感知装置、無線監視カメラなどの無線デバイスが原因の場合があります。

注記

上記 3 つの測定値の要約は、オートテスト機能でも示されています。

ネットワークのセキュリティー･リスクについて

❑ **ネットワークのセキュリティー･レベルは十分か？**

[ネットワーク] を選択します。安全でないアクセス･ポイントのあるネットワークは、赤色のアンロック･アイコン ( ) が表示されます。

❑ **エリア内にアドホック･ネットワークがあるか？**

[ネットワーク] を選択します。アド･ホック･ネットワーク･モードで作動しているステーションは、SSID 列にアド･ホック･アイコン ( ) が表示されます。アド･ホック･ステーションは、ネットワーク･セキュリティーにとってリスクになることも、ネットワーク･ポリシーに違反する原因となることもあります。

オートテストでは、アド･ホック･ネットワーク･テストが実行され、アド･ホック･ステーションにフラグが付きます。

- ❑ **エリア内に不正アクセス･ポイントがあるか？それらはどこにあるか？**

  AirCheck を使用すると、検出されたアクセス･ポイントの承認ステータスを追跡できます。デフォルトでは、アクセス･ポイントが検出されると、それらに承認ステータス ? **(不明)** が割り当てられます。アクセス･ポイントのステータスを個別に、またはグループ単位で変更し、ネットワークとの関係 (承認済み、近接、未承認など) を反映させることができます。

  また、デバイスのデフォルト･ステータスを ? **(不明)** から ✓ **(承認済み)** に変更することもできます。変更すると、検出されたすべてのアクセス･ポイントが ✓ **(承認済み)** として識別されます。その後、リストを確認して、個々のアクセス･ポイントにステータスを適切に割り当てることができます。例えば、アクセス･ポイントが不正であることがわかっている場合は、そのアクセス･ポイントに **(フラグ付きデバイス)** または ⚠ **(未承認デバイス)** のステータスを指定できます。

  デフォルトのデバイス承認ステータスを指定するには、**[ツール] > [Set Device Authorization (ACL) default (デバイス承認 (ACL) のデフォルトを設定)]** を選択します。

  特定のアクセス･ポイントまたはアクセス･ポイントのグループに承認ステータスを指定するには、**[アクセス･ポイント]** を選択し、アクセス･ポイントを反転表示してから、F2 **[ACL]** を押します。

すべてのアクセス･ポイントの承認ステータスを ✓ **(承認済み)** に設定するには、✓**[Set All APs to Authorized (すべての AP を承認済みに設定)]** を選択します。これにより、検出されたすべてのアクセス･ポイントが ✓ **(承認済み)** としてマークされます。この方法を使用して、デフォルトの承認ステータスを ? **(不明)** に設定した場合は、新たに検出されたアクセス･ポイントが ? **(不明)** として表示されます。一般的に、この方法を使用すると、セキュリティー･リスクや新しいアクセス･ポイントをすばやく調べることができます。

AP BSSID/MAC またはベンダー MAC プレフィックスに基づいて、一連の AP を承認済みまたは未承認に設定することもできます。それには、✓**[Set AP series to Authorized (一連の AP を承認済みに設定)]** または ⚠**[Set AP series to Unauthorized (一連の AP を未承認に設定)]** を選択します。これらのオプションを使用すると、設定時間を短縮し、潜在的な問題点をすばやく調べることができます。例えば、特定のベンダーの機器がネットワーク･ポリシーに従って拒否されている場合は、ベンダー MAC プレフィックスを使用して、ACL を未承認に設定します。これにより、該当するアクセス･ポイントが検出されると、自動的に未承認として報告されます。

注記

プロファイルを保存すると、割り当てられた ACL もこのプロファイルの一部として保存されます。

オートテストには、オプションとして、不正アクセス･ポイントを検出および報告する不正アクセス･ポイント･テストが含まれています。この機能を有効にするには、**[ツール] > [Thresholds / AutoTest Settings (しきい値 / オートテストの設定)] > [Rogue Access Point AutoTest (不正アクセス･ポイントのオートテスト)]** を選択します。正確で意味のあるテスト結果を得るには、オートテストを実行する前にアクセス･ポイントの ACL を設定しておく必要があります。

アクセス･ポイントの特定方法

[アクセス･ポイント] を選択し、アクセス･ポイントを 1 つ選択してから、**[アクセス･ポイントの詳細]** 画面で F2 **[場所の特定]** を押します。オプションのフルーク･ネットワークス製外付け指向性アンテナを使用して、アクセス･ポイントの検出時間を短縮することもできます。

マイ･ネットワークおよびマイ･テスト･セッションの記録方法

セッションを保存 (を押す) してから、AirCheck マネージャー･ソフトウェアを使用して PC にデータをダウンロードし、レポートを作成します。

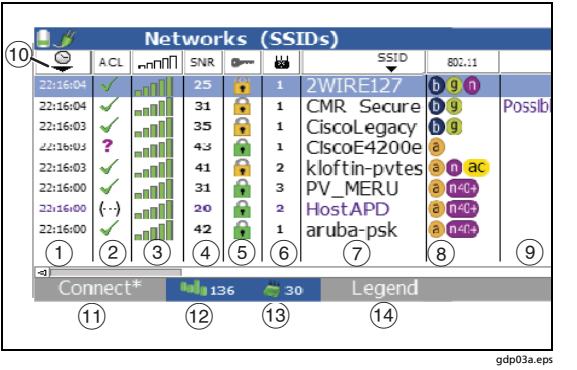
AirCheck のすべての情報を消去する方法

テスターからすべての設定、セッション･データ、プロファイルを消去するには、**[ツール] > [Erase All (すべて消去)]** を選択します。AirCheck テスターに保存または格納されている情報がすべて消去されます。

チャネル、ネットワーク、AP、またはクライアントの検出

チャネル、ネットワーク、アクセス･ポイント、またはクライアントを検出するには、ホーム画面で **[チャネル]**、**[ネットワーク]**、**[アクセス･ポイント]**、または **[クライアント]** を選択します。図 2 は **[ネットワーク]** リストを示します。

ネットワークまたはアクセス･ポイントの詳しい情報を表示するには、 を使用してネットワークまたはアクセス･ポイントを反転表示にしてから、 を押します。



gdp03a.eps

図 2. [ネットワーク] リスト

① : テスターが初めてネットワークを認識した時刻。あるエリア内を移動中に、その範囲内に入ってくるネットワークを表示するには、タイムスタンプの列を基準にしてリストを降順に並べ替えます。

を押して、エリア内を移動します。範囲に入ってきたネットワークは、リストの一番上に追加されます。範囲外になったネットワークは、**[検出できないアクセス･ポイントをグレー表示する]** が有効な場合、グレー表示されます。

② **ACL:** アクセス･ポイントの承認ステータス。デフォルトのステータスは **?** **(不明)** ですが、✓ **(承認済み)** に変更できます。各アクセス･ポイントのステータスを変更して、ネットワークとの関連性を表示します。ステータスを変更するには、ホーム画面で **[アクセス･ポイント]** を選択し、アクセス･ポイントを選択して、 F2 **[ACL]** を押します。

(...): ネットワーク内のすべてのアクセス･ポイントが同じ承認ステータスではありません。

③ ▁▃▅▇: ネットワーク SSID のすべてのアクセス･ポイントの最大信号強度。

④ **SNR:** 信号対ノイズ比のレベルは、ノイズに対する信号強度比率の測定値です。この比率はデシベル (dB) で測定されます。

⑤ 🔑: ネットワークのセキュリティー･ステータス。
🔓アンロック･アイコン (赤): ネットワークのセキュリティーが有効になっていません。

注記

アンロックされているネットワークの中には、テスターを接続して、Ping テストなどの測定を実行できるものもあります。ただし、同じネットワークに接続されている PC を、ユーザー ID およびパスワードを指定しないで Web に接続することはできません。

ロック･アイコン (黄): 1 つ以上のアクセス･ポイントで WEP または Cisco LEAP セキュリティー･プロトコルが使用されています。これらの安全性は他のプロトコルよりも低くなります

ロック･アイコン (緑): すべてのアクセス･ポイントが、WEP よりも安全性の高いセキュリティー･プロトコル (WPA、WPA2 など) を使用しています。

(...): ネットワーク内のアクセス･ポイントの中に、異なるタイプのセキュリティーを使用しているものがあります。例えば、あるアクセス･ポイントでは WEP、別のアクセス･ポイントでは WPA が使用されています。

⑥ : ご使用の場所でテスターが認識しているアクセス･ポイント数。

⑦ **SSID**: サービス･セット識別子。無線ネットワークの名前です。

: ネットワーク内にアド･ホック･デバイスがあります。これは、ネットワークの一部であるアクセス･ポイントを介さず、他のデバイスと直接通信するデバイスです。アド･ホック･デバイスがあると、ハッカーはネットワーク上で送信されるデータにアクセスできるようになります (ネットワークの IT ポリシーによっては、アド･ホック･デバイスが許可されている場合があります)。

[非表示]: ネットワークは、その SSID を送信しません。

⑧ **802.11**: ネットワーク内のアクセス･ポイントが使用する 802.11 規格。

802.11a: 5 GHz の帯域を使用。

802.11b: 2.4 GHz の帯域を使用。

g 802.11g: 2.4 GHz の帯域を使用。

n 802.11n: 2.4 GHz または 5 GHz の帯域を使用。

ac 802.11ac: 5 GHz の帯域を使用。

赤色のバー : テスターが、**[ツール]** > **[国設定]** の設定と異なる国コードを受信しました。この国コードを送信しているネットワークやアクセス・ポイントを特定するには、**[ネットワーク]** または **[アクセス・ポイント]** を選択し、**[802.11]** 列で赤いバーを探します。

n40+ n40– : 1つまたは複数のアクセス・ポイントが結合チャネルを使っています。802.11n 規格を使用するアクセス・ポイントは、あるチャネルとその上 (n40+) または下 (n40–) の拡張チャネルを結合して、1 つの 40 MHz チャネルにすることができます。チャネル幅が広いほど、ネットワークのスループットが高くなります。

(...): ネットワーク内のアクセス・ポイントのうち、同じ802.11規格を使用していないものがあります。

⑨ **メモ**: ▷ を押して、メモ・フィールドまでスクロールします。テスターは自動的にメモを追加します。メモのあるネットワークは紫色で表示されます。

(...): ネットワークには複数のメモがあります。すべてのメモを表示するには、ネットワークを反転表示してから SELECT を 2 回押して、**[アクセス・ポイントの詳細]** 画面に移動します。

⑩ ▼ ▲ : **[並べ替え 1]**、降順および昇順

▼ ▲ : **[並べ替え 2]**、降順および昇順

一覧を昇順または降順で並べ替えるには、▲▼ および ◀ ▶ を使用して列見出しを反転表示してから、SELECT または F1 **[並べ替え 1]** を押します。例えば、最も強い信号を持つアクセス･ポイントをすばやく見つけるには、列の上部にある ▁▂▃▅▇ を反転表示してから、SELECT または F1 **[並べ替え 1]** を押します。これにより、最も強い信号を持つアクセス･ポイントが一覧の最上部に表示されます。

2 番目の基準で並べ替えるには、別の列見出しを反転表示してから、F2 **[並べ替え 2]** を押します。

⑪ 反転表示されたネットワークに接続するには、F1 **[接続]** を押します。

反転表示されたネットワークにテスターが接続できない場合は、ボタンが **[接続 *]** (アスタリスク付き) と表示されます。ネットワークのセキュリティー設定を行うには、F1 **[接続 *]** を押します。

注記

安全なネットワークに接続するには、テスターにセキュリティー証明書を含むプロファイルが必要です。セキュリティー証明書の作成または編集は、テスターで行うか、AirCheck Manager を使用して行います。テスターの [接続 *] を押すと、セキュリティー設定手順がガイドされます。[ツール] をクリックしてから [Manage profiles / network passwords (プロファイル/ネットワーク･パスワードの管理)] をクリックして、セキュリティーを再設定することもできます。[接続] の右にある * は、セキュリティー設定が行われていないことを示しています。[接続] を使用してセキュリティーを設定する手順については、ユーザーズ･マニュアルを参照してください。

⑫ : テスターが現在モニターしているチャネル。バーの色は規制領域に対する国コードのステータスを示します。

⑬ : ご使用の場所でテスターが認識しているアクセス･ポイント数。**[仮想アクセス･ポイントをグループ化する]** が選択されている場合、仮想アクセス･ポイントはこの数に含まれません。

⑭ **[ネットワーク]** 画面上のアイコンの詳細を確認するには、F2 **[凡例]** を押します。

ネットワーク内のアクセス･ポイントの詳細を確認するには、▲ ▼ を使用してネットワークを反転表示してから、SELECT を押します。

FLUKE networks

AirCheck™

Wi-Fi 测试仪

入门指南

PN 3434814 12/2009 Rev. 4, 8/13 (Simplified Chinese)
©2009-2013 Fluke Corporation. Printed in USA.
All product names are trademarks of their respective companies.
Wi-Fi® is a registered trademark of the Wi-Fi Alliance.

有限保修和责任限制条款

Fluke Networks 保证，自购买之日起一年内，本产品不会出现材料和工艺等方面的缺陷。除非另行说明，否则部件、附件、产品维修和维护的保证期限为 90 天。镍镉、镍氢和锂离子电池、电缆或其他外围设备都将视为部件或附件。

本保修不包括因意外、疏忽、误用、改装、污染及非正常操作或处理而造成的损坏。经销商无权以 Fluke Networks 的名义增加其他任何保修。

欲在保修期内取得保修服务，请与距离您最近的 Fluke Networks 授权服务中心联系，以获取运回授权信息，然后将有问题的产品寄到该维修中心，并随附产品的问题说明。

本保修是您唯一可以获得的补偿保证。不做任何明示或暗示的其他担保（例如适用于特定目的的暗示担保）。FLUKE NETWORKS 不负责承担任何特殊、间接、偶然或顺带损坏或损失，无论是出于何种原因或理论。

由于某些州或国家/地区禁止排除或限制暗示担保的条款，或者禁止排除或限制偶然或顺带损坏，因此本保修中的责任限制和排除条款可能对您不适用。

4/04

Fluke Networks
PO Box 777
Everett, WA 98206-0777
USA

目录

查看用户手册 1
警告信息 2
一般规格 4
维护、保养和设备免受损保护 5
联系 Fluke Networks 6
电池充电和使用时间 7
主屏幕 8
采用最低配置实现最佳性能 11
您对无线网络有哪些了解？ 12
我的网络的健康状况如何？ 12
无线 LAN 中有什么？ 15
设备是否能连接到无线网络？ 16
导致网络性能变慢或连接中断的原因是什么？ 17
网络中是否存在安全风险？ 18
如何定位接入点？ 20
如何记录我的网络以及我的测试会话？ 20
如何清除 AirCheck 上的所有数据？ 20
发现信道、网络、接入点或客户端 21

查看用户手册

本指南提供的基本信息能帮助您逐步了解如何使用 AirCheck™ Wi-Fi 测试仪。有关更多信息，请参阅产品 CD 中的用户手册。

产品 CD 还包含 AirCheck Manager 应用程序，帮助您最有效地使用测试仪。

警告信息

AirCheck ™ Wi-Fi 测试仪是专门用于快速验证 Wi-Fi 网络并排除其故障的手持式工具。

⚠警告⚠

使用产品前请仔细阅读全部安全须知。

仅按照规定使用产品，否则可能会降低产品本身自带的保护能力。

请仔细阅读全部说明。

仅使用 Fluke 批准的电源适配器为电池充电。

切勿在爆炸性气体、蒸汽周围或潮湿的环境中使用产品。

使用产品前检查包装箱是否开裂或残缺，仔细查看端子周围的绝缘材料。

电池含有危险化学物，可能会燃烧或爆炸。如果接触到化学物，立即用清水洗净并就医。

如果产品放置较长一段时间不用或存储温度高于 50 °C，请取出电池。如果不取出电池，电池漏电将损坏产品。

请勿让电池端子同时短路。

请勿拆卸或挤压电池和电池组。

请勿将电池和电池组放在热源或火源附近。不可接受阳光照射。

未使用时请勿连续为电池组充电。

请勿使电池组遭受机械冲击。

请勿打开电池组，里面没有可由用户自行维修的部件。

请参阅《产品手册》中关于为电池组充电的相关说明。

为了避免引起火灾、触电、人身伤害或测试结果不准确，请先阅读 *AirCheck 用户手册*中的安全须知，然后再使用测试仪。

	警告或注意：有损坏或毁坏设备或软件的风险。请参见手册中的解释。
	警告：有电击的危险。
	请勿将包含电路板的产品扔进废物箱。请参阅当地有关处理流程的法规。
	本设备包含一个 2 级无线电。
	符合相关的欧盟指令。
	符合 FCC 规则， 15.107、 15.109 部分。
	通过加拿大标准协会认证。
	符合相关的澳大利亚标准
	符合相关的韩国 EMC 标准。

其他韩国 EMC 标准信息：

电磁兼容性。仅适用于在韩国使用时的情况。A 类设备 （工业广播和通信设备） [1]	[1] 销售员和使用者必须注意此产品符合工业 （A 类）电磁波设备的要求。此设备适用于工作环境，不适用于家用。

一般规格

电池类型：可插拔充电式锂离子电池组 （18.5 瓦时）

工作温度和相对湿度：32°F 至 113°F （0°C 至 +45°C）

工作相对湿度：（% RH 无冷凝）90%（50°F 至 95°F；10°C 至 35°C） 75% （95°F 至 113°F；35°C 至 45°C）

存放温度：-4°F 至 140°F （-20°C 至 +60°C）

撞击和震动：随机，2 g，5 Hz-500 Hz（2 类）1 米跌落测试

海拔：4000 m；**存储海拔**：12000 m

安全：IEC/EN 61010-1

维护、保养和设备免受损保护

· 电池是唯一可由用户维修的部件。除非更换电池，否则不得打开电池盒。

· 仅使用 Fluke Networks 批准的备用零部件。

· 如果未按照制造商规定的方式使用本设备，设备提供的保护可能会遭到破坏。

· 清洁外壳时，请使用沾有水或水与温和清洁剂的湿润软布。

联系 Fluke Networks

www.flukenetworks.com
support@flukenetworks.com
+1-425-446-4519

- 澳大利亚：61 (2) 8850-3333 或 61 (3) 9329 0244
- 北京：86 (10) 6512-3435
- 巴西：11 3759 7600
- 加拿大：1-800-363-5853
- 欧洲：+31-(0) 40 2675 600
- 香港：852 2721-3228
- 日本：03-6714-3117
- 韩国：82 2 539-6311
- 新加坡：+65-6799-5566
- 台湾：(886) 2-227-83199
- 美国：1-800-283-5853

请访问我们的网站，获取完整的电话号码表。

电池充电和使用时间

首次使用电池前，应充电 **4** 小时。请将交流电源适配器连接到 **AirCheck** 测试仪上的电池接头为电池充电。

典型操作期间，电池可使用约 **5.5** 小时。

显示电池状态。电池电量低时，该图标闪烁。

显示交流电源适配器已连接。

主屏幕

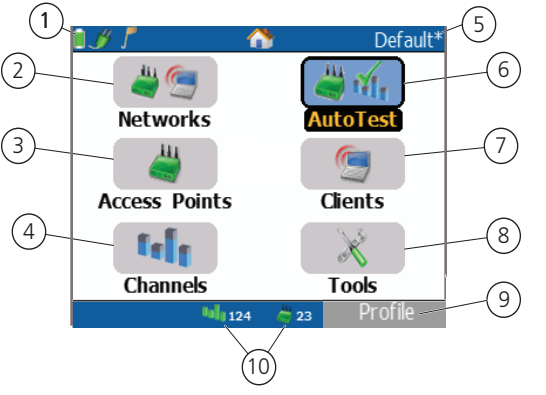


图 1. 主屏幕组件

① 显示电池状态。电池电量低时，该图标闪烁。连接交流电源适配器为电池充电，确保测试仪持续工作。

显示交流电源适配器已连接。

显示外部天线已连接。

注意

连接外部天线时，AirCheck 不会传输或连接至某个接入点。

② **网络**：发现无线 LAN。

③ **接入点**：发现接入点。

④ **信道**：显示 WLAN 信道的利用率。

⑤ 测试仪当前使用的配置文件的名称。如果您未加载其他配置文件，则当前的配置文件为默认文件。如果您加载或保存该配置文件后更改了测试仪上的某项设置，则名称会显示一个星号。

⑥ **自动测试**：通过查看空气质量 （信道利用率和干扰）、网络质量 （网络覆盖率和连接性），自动检查网络的健康状况，以及是否存在自组网络。

⑦ **客户端**：发现使用您网络的客户端。

⑧ **工具**：用于管理文件和设置。

⑨ **配置文件**：显示可用配置文件的列表。

⑩ 左侧：

测试仪当前监控的信道。信号条形图的颜色表示调节域的国家/地区代码。红色图标表示为当前的国家/地区设置运行非法信道和/或收到其他国家/地区代码。

右侧：

测试仪侦听到的物理接入点的数量。

测试仪上的接入点数据库最多可存储 500 个接入点。接入点图标变黄就表示发现 400 个或更多接入点。

该图标变红则表示发现 500 个或更多接入点，且接入点数据库已满。列表中将不会列出任何新发现的接入点。

采用最低配置实现最佳性能

更改语言和国家/地区设置

1 选择**工具**。

2 如要更改屏幕显示的语言，请选择**设置语言**。突出显示某种语言，然后按下 F2 **保存**。

3 如要更改国家/地区，请选择**设置国家/地区**，然后选择使用该测试仪时所在的国家/地区，按下 F2 **保存**。

如要实现测试仪的最佳性能，请使用 AirCheck™ Manager 软件对配置文件进行配置并将其加载到测试仪。配置文件还可在 AirCheck 测试仪上配置，并包含测试者用于执行以下任务的数据：

- 连接到需要安全凭证的网络。
- 显示各个接入点正确的授权状态。这样，您就可以快速查看哪些接入点是网络的授权接入点。
- 使用 Ping 命令测试关键网络设备。
- 使用主机名称或 IP 地址和指定的端口号，运行 TCP 端口连接测试。

您对无线网络有哪些了解？

我的网络的健康状况如何？

- ❑ **我的 Wi-Fi 环境质量如何？**
  我的信道的接入点和 Wi-Fi 流量是否过载？
  是否有信道噪音过大？

  选择**自动测试。**自动测试运行后，选择**环境质量**，查看 802.11 信道利用率、非 802.11 信道利用率以及同信道干扰健康状况评估的结果。

  802.11 信道利用率结果包括前三个 Wi-Fi 流量最多、最繁忙的信道。显示信道利用率的值和评级：✓（成功）、⚠（警告）或 ✗（失败）。测试等级基于实际数值与用户设定阈值进行的比较而确定。在**工具 > 阈值/自动测试设置**中设置阈值。

  802.11 信道利用率结果包括非 802.11 干扰和噪音最大的前三个信道。显示信道利用率的值和评级：✓（成功）、⚠（警告）或 ✗（失败）。

  同信道干扰结果包括接入点信号强度和信号质量最低的前三个信道。显示接入点数量和评级：✓（成功）、⚠（警告）或 ✗（失败）。

- **我的 Wi-Fi 网络质量如何？**
  是否能侦听到支持我的网络的任何接入点？
  此区域内是否存在覆盖漏洞？
  是否有过多邻近的接入点使用同一信道从而导致网速变慢？
  是否能够连接？

  选择**自动测试** - 自动测试运行后，选择**网络质量**，查看覆盖范围、同信道干扰、安全和连接性健康状况评估的结果。

  覆盖范围结果包括用于支持网络 (SSID) 的信号质量良好 （指信号强度良好和信噪比良好）的接入点数量，同时显示评级：✓（成功）、⚠（警告）或 ✗（失败）。测试等级基于实际数值与用户设定阈值进行的比较而确定。在**工具 > 阈值/自动测试设置 > 接入点覆盖范围，信号等级**和**信噪比阈值**屏幕上设定接入点数量、信号等级和信噪比的信号质量阈值。

  同信道干扰结果基于网络和阈值的比较而得出，包括网络重叠接入点的数量，同时显示评级：✓（成功）、⚠（警告）或 ✗（失败）。在**工具 > 阈值/自动测试设置 > 网络质量同信道阈值**屏幕上设定此测试的阈值。

  安全结果将报告 SSID 上的所有接入点是否使用相同的安全凭证，并显示评级：✓（成功）、⚠警告）或 ✗（失败）。

  连接性测试尝试连接到配置文件中配置的各个网络。连接性测试结果表明您是否连接到所在位置的网络，同时显示测试等级：成功或失败。有关连接的其他详情，例如信道、接收到的 IP 地址、连接速率等，以评级形式显示：✓（成功）、⚠（警告）或 ✗（失败）。

- **有哪些未经授权或未知的接入点连接到我的 Wi-Fi 网络？**
  这些接入点是否有安全风险？

  恶意接入点测试是自动测试的可选内容，以评级形式 ✓（成功）、⚠（警告）或 ✗（失败），表明是否检测到未经授权或未知的接入点。结果包含在您所在位置侦听到的所有恶意接入点列表中。如要识别恶意接入点，需要配置访问控制列表 (ACL)。可在自动测试屏幕上配置 ACL，方法是依次选择**恶意接入点 > ACL** 或**主页> 接入点 > ACL**。

无线 LAN 中有什么？

- ❑ **哪些无线 LAN 可用？**

  选择**网络**查看无线 LAN 列表以及连接到各网络的接入点。如要查看您所在位置可用的所有接入点，请选择**接入点**。

- ❑ **哪些接入点可用？信号强度是否充足？**

  选择**接入点**查看您所在位置可用的接入点列表以及接入点的信号强度。如要查看信号强度的条形图以及接入点的噪音，请突出显示该接入点，然后按下 SELECT。

- ❑ **接入点的配置是否正确？**

  在主屏幕上，选择**接入点**，突出显示某个接入点，然后按下 SELECT。

- ❑ **该区域内是否有新的接入点？这些接入点是您的接入点，还是相邻接入点，又或者是恶意接入点？**

  在您的所在位置发现新的接入点时，使用设备授权状态 (ACL) 功能自动报告。如要使用此功能，请配置各接入点的授权状态 （例如授权或相邻），然后将默认授权状态设为 **？ 未知**。默认授权状态 **？ 未知**便会分配给之前未发现的任何接入点。最后，从主屏幕中选择**接入点**，查看是否将所有接入点标记为 **？ 未知**。

  或者，您也可以保存包含已发现接入点列表的测试会话。使用 AirCheck Manager 将接入点列表与之前保存的会话文件进行比较，查看是否发现了其他接入点。

  如要将默认设备的授权状态指定为未知或授权，请选择**工具 > 将设备授权状态 (ACL) 设为默认**

❑ **哪些无线客户端使用该网络？**

从主屏幕中，选择**客户端**。您还可以深入了解接入点或信道详细信息，查看相关客户端列表。

设备是否能连接到无线网络？

使用测试仪检验连接性。

❑ **设备是否能作为客户端连接到网络 (SSID)？**

选择**网络**，突出显示某个网络，然后按下 F1 **连接**。

注意

如要连接到安全网络，测试仪必须安装有包含安全凭证的配置文件。

❑ **设备是否能连接到接入点 (BSSID)？**

选择**接入点**，突出显示某个接入点，然后按下 F1 **连接**。如果**连接**右侧显示 *****，则表示测试仪上未配置该网络的安全性。按下**连接***后，系统会指导您输入安全设置。设置后，将该设置保存到当前的配置文件。依次按下**工具和管理配置文件/网络密码**，重新编辑安全设置 （如果需要）。

❑ **如果设备无法连接到网络或接入点，则连接流程的哪个环节出了问题？**

查看连接日志。从**连接到网络或连接到接入点**屏幕中按下 F2 **日志?**

❑ **设备是否能使用 Ping 命令测试网络设备？**

使用 Ping 命令测试。连接到某个网络或接入点，然后按下 F1 **开始测试**。

注意

*依次选择**工具 > 管理配置文件\网络密码 > 编辑对象 > 添加**，即可添加 Ping 对象。您可通过 IP 地址或主机名称 (URL) 添加对象。*

*如果**连接**右侧显示 *****，则表示测试仪上未配置该网络的安全性。按下**连接***后，系统会指导您输入安全设置。*

- ❑ **客户端中的网络接口卡运行是否正常？**

  选择**客户端**，然后查看 SSID 列。带虚线的 SSID 为探测客户端，显示 SSID 名称的客户端为关联客户端。按下 (SELECT)，查看客户端是否传输探测请求帧。

导致网络性能变慢或连接中断的原因是什么？

- ❑ **信号强度是否充足？**

  选择**接入点**。**接入点**屏幕显示各接入点的信号强度。选择其中一个接入点，查看其信号强度和拥塞的更多详情。

- ❑ **网络是否太忙？**

  选择**信道**，查看信道使用情况概况以及使用各信道的接入点数量。要查看图表，请突出显示某个信道，然后按下 (SELECT)。

- ❑ **信道上是否存在非 802.11 干扰？**

  选择**信道**。非 802.11 干扰显示为灰色。此噪音会干扰 WLAN 的连接或性能。非 802.11 噪音来自于微波炉、无线电话、 Bluetooth® 设备、移动探测器、无线摄像机及其它无线设备。

注意

***自动测试**功能还将汇总之前三次的测量结果。*

网络中是否存在安全风险？

- ❑ **网络是否有预期的安全级别？**

  选择**网络**。拥有不安全接入点的网络显示红色锁图标 ( )。

- ❑ **该区域内是否存在任何自组网络？**

  选择**网络**。在自组网络模式下运行的站点将在 SSID 栏中显示"自组"图标 ( )。自组站点会对网络安全构成风险，也会违反网络策略。

  自动测试包括自组网络测试，用于标出自组站点。

- ❑ **该区域内是否存在恶意接入点？这些接入点的位置在哪里？**

  AirCheck 可用于帮助跟踪已发现的接入点的授权状态。默认情况下，发现接入点时，会向其分配 ? **未知**授权状态。您可更改单个接入点或一组接入点的状态，反映它们与您网络的关系，例如授权、邻近、未经授权。

  您还可选择将默认设备状态从 ? **未知**更改为 ✓ **授权**。更改后，所有发现的接入点将被识别为 ✓ **授权**。然后，您可查看列表并将状态相应分配至各个接入点。例如，如果您知道某个接入点为恶意接入点，则可向其分配状态 **已标记设备**或 ⚠ **未经授权设备**。

  如要指定设备授权状态为默认，请选择**工具 > 将设备授权状态 (ACL) 设为默认**。

  如要指定某个接入点或一组接入点的授权状态，请选择**接入点**，突出显示某个接入点，然后按下 F2 **ACL**。

您可将所有接入点的授权状态设为 ✓ **授权**，方法是选择 ✓ **将所有接入点设为授权**。这样，便可将所有发现的接入点标记为 ✓ **授权**。使用此方法，将默认授权状态设为 ? **未知**时，新发现的接入点便会显示为 ? **未知**。总的来说，使用这种方法，可快速显示安全风险或新的接入点。

您还可根据 AP BSSID/MAC 或供应商 MAC 地址前缀，将一系列接入点的状态设为授权或未经授权，方法是选择 ✓ **将接入点系列的状态设为授权**或 ⚠ **将接入点系列的状态设为未经授权**。这些选项可节约您的配置时间，并让您快速发现潜在问题。例如，如果根据您的网络策略不允许使用特定供应商提供的设备，则使用供应商 MAC 地址前缀将 ACL 设定为未经授权。一旦检测到这些接入点时，系统会自动报告为未经授权的接入点。

注意

保存您的配置文件时，分配的 ACL 也将作为该配置文件的一部分保存。

自动测试还可包含恶意接入点测试，检测并报告恶意接入点。如要启用此功能，请转至**工具 > 阈值/自动测试设置 > 恶意接入点自动测试**。为了获取精确、有意义的测试结果，必须先配置接入点 ACL，然后再运行自动测试。

如何定位接入点？

选择**接入点**，选中某个接入点，然后在**接入点详情**屏幕上按下 F2 **定位**。您还使用选配的 Fluke Networks 外置定向天线，帮助您更快发现接入点。

如何记录我的网络以及我的测试会话？

保存会话 （按下 💾），然后使用 AirCheck Manager 软件将数据下载到 PC 上，并制作报告。

如何清除 AirCheck 上的所有数据？

如果您想要清除测试仪上的所有设置、会话数据和配置文件，请选择**工具 > 清除所有**，便可清除 AirCheck 测试仪上保存或存储的所有内容。

发现信道、网络、接入点或客户端

如要发现信道、网络、接入点或客户端，请在主屏幕上选择**信道**、**网络**、**接入点**或**客户端**。图 2 显示的是一个**网络**列表。

如要查看有关某个网络或接入点的详细信息，请使用 ◄► 突出显示该网络或接入点，然后按下 SELECT。

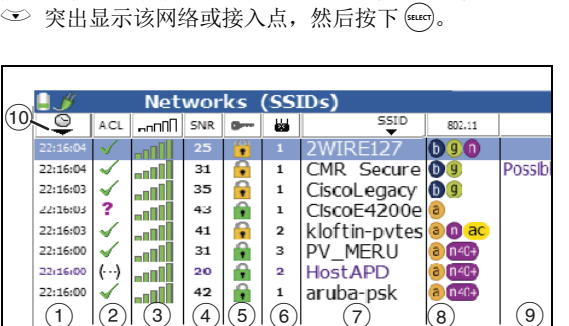


图 2. 网络列表

① : 测试仪首次侦听到网络的时间。如要查看您在区域内移动时进入覆盖范围的网络，则按降序排列时间戳列的列表。

按下 ，然后在区域内移动。进入覆盖范围的网络会添加到列表顶部。如果启用侦听不到的显示为灰色的接入点，**则网络将不在覆盖范围内并且**变灰。

② **ACL**：接入点的授权状态。默认状态为 **? 未知**，但可更改为 **✓ 授权**。将各接入点的状态更改为显示与网络关联的方式。如要更改此状态，请从主屏幕中选择**接入点**，选择其中一个接入点，然后按下 F2 **ACL**。

(...)：网络中所有接入点的授权状态并非都相同。

③ ⊓⊓⊓⊓：网络 SSID 所有接入点的最大信号强度。

④ **SNR**：信噪比水平用于测量信号强度与噪音的比值。该比值单位为分贝 (dB)。

⑤ 🔑：网络的安全状态：

🔓 红色开锁：网络未启用安全功能。

注意

某些显示开锁图标的网络允许您连接测试仪并执行包括运行 Ping 测试在内的测量，但可能不允许在不输入用户 ID 和密码的情况下将连接至同一网络的 PC 连接到 Web。

🔒 黄色闭锁：一个或多个接入点使用 WEP 或 Cisco LEAP 安全协议。这些协议的安全性比其他协议低。

🔒 绿色闭锁：所有接入点使用比 WEP 更安全的安全协议，例如 WPA 或 WPA2。

(...)：网络中的所有接入点使用不同的安全类型。例如，一个使用 WEP，另一个使用 WPA。

⑥ 📶：测试仪在您所在的位置侦听到的接入点数量。

⑦ **SSID**：服务集标识符。无线网络的名称。

：网络拥有临时设备。这些设备直接与其他设备通信，而不通过接入点进行通信。临时设备方便黑客访问网络上传输的数据。（某些网络 IT 策略允许使用临时设备。）

[隐藏]：网络不广播其 SSID。

⑧ **802.11**：网络中的接入点使用的 802.11 标准：

802.11a：使用 5 GHz 频段。

802.11b：使用 2.4 GHz 频段。

802.11g：使用 2.4 GHz 频段。

802.11n：使用 2.4 GHz 或 5 GHz 频段。

802.11ac：使用 5 GHz 频段。

红色条形图：测试仪收到的国家/地区代码不同于**工具 > 设定国家/地区**中的设置。如要识别传输该代码的网络或接入点，请选择**网络**或**接入点**，然后查找 **802.11** 列中的红色条形图。

n40+ n40–：一个或多个接入点使用一个捆绑信道。使用 802.11n 标准的接入点将信道与高于 (n40+) 或低于 (n40–) 的扩展信道捆绑，形成一个 40 MHz 信道。信道越宽，网络吞吐量就越高。

(...)：网络中的所有接入点并非都使用相同的 802.11 标准。

⑨ **注释：**按下 ▷ 滚动至注释字段。测试仪会自动添加注释。带注释的网络显示为紫色。

(...)：网络有多个注释。如要查看所有注释，突出显示该网络，然后按下 SELECT 两次转至**接入点详情屏幕**。

⑩ **排序方式 1**，降序和升序。

▼ ▲：**排序方式 2**，降序和升序。

如要以升序或降序对列表进行排序，请使用 ◁▷ 和 ◁▷ 突出显示列标题，然后按下 SELECT 或 F1 **排序方式 1**。例如，如要快速找到信号最强的接入点，请突出显示列顶部的 ▁▂▃▄▅，然后按下 SELECT 或 F1 **排序方式 1**。这样，便可将信号最强的接入点置于列表顶部。

如要以第二种方式排序，请突出显示另一个列标题，然后按下 F2 **排序方式 2**。

⑪ 按下 F1 **连接**连接到突出显示的网络。

如果测试仪无法连接至突出显示的网络，则连接按钮显示为**连接***（带星号）。如要配置网络的安全设置，请按下 F1 **连接***。

注意

*如要连接至安全的网络，测试仪必须安装有包含安全凭证的配置文件。在测试仪上创建或编辑安全凭证，或使用 AirCheck Manager。按下测试仪上的**连接***时，系统会指导您进行安全配置。您还可依次按下**工具**和**管理配置文件**/**网络密码**，重新配置安全设置。**连接**右侧的 * 表示尚未配置任何安全设置。请参阅《用户手册》，了解使用"连接"设置安全的流程。*

⑫ ：测试仪当前监控的信道。信号条形图的颜色表示调节域的国家/地区代码状态。

⑬ ：测试仪在您所在的位置侦听到的接入点数量。如果选择对**虚拟接入点**进行分组，则此数量不包括虚拟接入点。

⑭ 如要查看**网络**屏幕上图标的说明，按下 F2 **图例**。

如要查看网络中接入点的详细信息，使用 ◁ ▷ 突出显示某个网络，然后按下 SELECT。

FLUKE networks

AirCheck™

Wi-Fi 테스터

사용 시작 설명서

PN 3434814 12/2009 Rev. 4, 8/13 (Korean)
©2009-2013 Fluke Corporation. Printed in USA.
All product names are trademarks of their respective companies.
Wi-Fi® is a registered trademark of the Wi-Fi Alliance.

제한적 품질 보증 및 배상 책임의 제한

Fluke Networks는 본 제품이 구입일로부터 1년 동안 재료와 제작상에 하자가 없음을 보증합니다. 별도로 명시되지 않는 한, 부품, 부속품 및 제품의 수리와 정비는 90일 동안 보증됩니다. 니켈 카드뮴, 니켈 수소 및 리튬 이온 배터리, 케이블 또는 기타 주변 기기는 모두 부품 또는 부속품으로 간주됩니다.

사고, 설명서 무시, 오용, 개조, 오염 또는 비정상인 작동이나 취급으로 제품이 손상되었다고 판단되면 본 품질 보증이 적용되지 않습니다. 판매점은 이 외의 어떤 보증도 Fluke Networks를 대신하여 추가로 제공할 수 없습니다.

보증 기간 내에 품질 보증 서비스를 받으려면, 가까운 Fluke Networks 지정 서비스 센터에 문의하여 RMA(제품 반송 신청) 정보를 받은 다음, 문제점에 대한 설명과 함께 해당 서비스 센터로 제품을 보내시기 바랍니다.

본 보증은 구매자의 독점적이고 유일한 구제 수단이며, 특정 목적에 대한 적합성 같은 모든 다른 명시적, 암시적 보증을 대신합니다. Fluke Networks는 발생한 원인이나 이론에 상관없이 어떠한 특수한, 간접적, 부수적 또는 결과적인 손상이나 손실에 대해서도 책임을 지지 않습니다.

암시된 보증이나 부수적 또는 결과적인 손상을 제외하거나 제한하는 것을 금지하고 있는 일부 주나 국가에서는 이러한 배상 책임의 제한이 적용되지 않을 수 있습니다.

4/04

Fluke Networks
PO Box 777
Everett, WA 98206-0777
USA

목차

사용 설명서의 사용 1
경고 정보 2
  일반 사양 5
  유지 관리, 서비스 및 보호 장비 손상 6
Fluke Networks 연락처 7
배터리 충전 및 수명 8
홈 화면 9
최고의 성능을 위한 최소 구성 12
무선 네트워크에서 확인할 수 있는 사항 13
  내 네트워크의 상태는 어떻습니까? 13
  무선 LAN에는 어떤 것이 있습니까? 16
  장치를 무선 네트워크에 연결할 수 있습니까? 18
  네트워크 성능 저하 또는 연결 중단의 원인이 무엇입니까? 19
  네트워크에 보안 위험이 있습니까? 20
  액세스 지점을 어떻게 찾을 수 있습니까? 23
  내 네트워크 및 내 검사 세션을 어떻게 문서로 만들 수 있습니까? 23
  어떻게 하면 AirCheck의 모든 정보를 지울 수 있습니까? 23
채널, 네트워크, AP 또는 클라이언트 검색 24

사용 설명서의 사용

이 설명서는 AirCheck™ Wi-Fi 테스터를 처음 사용할 때 참조할 수 있는 기본 정보를 제공합니다. 자세한 정보는 제품 CD에 있는 사용 설명서를 참조하십시오.

또한, CD에는 테스터를 최대한 활용하는 데 도움을 주기 위한 AirCheck Manager 응용프로그램이 포함되어 있습니다.

경고 정보

AirCheck ™ Wi-Fi 테스터는 Wi-Fi 네트워크의 문제를 신속히 확인하고 해결하기 위한 휴대용 전용 도구입니다.

⚠경고⚠

제품을 사용하기 전에 안전 정보를 모두 읽으십시오.

지정된 방식으로만 제품을 사용하십시오. 그렇지 않으면 제품에서 제공하는 보호 기능이 손상될 수 있습니다.

모든 지침을 주의해서 읽으십시오.

배터리를 충전할 때에는 Fluke 인증 전원 어댑터만 사용하십시오.

주변에 가연성 가스 또는 증기가 있거나 습한 환경에서는 제품을 사용하지 마십시오.

제품을 사용하기 전에 케이스를 점검하십시오. 금이 갔거나 없어진 플라스틱이 있는지 확인하고, 터미널 주변의 절연 상태를 주의하여 살펴보십시오.

배터리에는 화상이나 폭발을 유발할 수 있는 유해한 화학물질이 포함되어 있습니다. 화학물질에 노출된 경우 물로 깨끗이 씻어낸 후 의사의 진료를 받으십시오.

장시간 제품을 사용하지 않거나 50 °C 이상의 온도에서 보관하는 경우 배터리를 분리하십시오. 배터리를 분리하지 않을 경우 배터리 누수로 제품이 손상될 수 있습니다.

배터리 터미널을 단락시키지 마십시오.

배터리 셀/팩을 분해하거나 파손하지 마십시오.

배터리 셀/팩을 열기나 화기 근처 또는 직사광선이 닿는 곳에 두지 마십시오.

사용하지 않는 배터리 팩을 계속해서 충전하지 마십시오.

배터리 팩에 기계적 충격을 가하지 마십시오.

배터리 팩을 열지 마십시오. 내부에 사용자가 취급할 수 있는 부품이 없습니다.

배터리 팩 충전에 관한 올바른 지침을 확인하려면 제품 명서를 참조하십시오.

화재, 감전, 부상, 장비 손상 또는 부정확한 검사 결과를 방지하려면 테스터를 사용하기 전에 ***AirCheck** 사용 설명서*의 안전 정보를 읽으십시오.

	경고 또는 주의: 장비나 소프트웨어의 손상 또는 파손 위험. 설명서를 참조하십시오.
	경고: 감전 위험
	회로판이 포함된 제품을 휴지통에 버리지 마십시오. 폐기 절차는 현지 규정을 참조하십시오.
	이 장비는 Class 2 라디오를 포함합니다.
	관련 유럽 연합 지침 준수
	FCC 규정, Part 15.107, 15.109 준수
	캐나다 표준 협회에 등록되어 있음
	관련 오스트레일리아 표준 준수
	관련 한국 EMC 표준 준수

추가 한국 EMC 표준 정보

A급 기기 **(업무용 방송통신기자재)**	**이 기기는 업무용 (A급) 전자파 적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는 것을 목적으로 합니다.**

일반 사양

배터리 타입: 교체 가능한 충전식 리튬 이온 배터리 팩 (18.5와트/시)

작동 온도 및 상대 습도: 0°C-+45°C(32°F-113°F)

작동 상대 습도: (% RH 비응축) 90%(10°C-35°C, 50°F-95°F), 75%(35°C-45°C, 95°F-113°F)

보관 온도: -20°C-+60°C(-4°F-140°F)

충격 및 진동: 무작위, 2g, 5Hz-500Hz(Class 2) 1m 낙하 검사

고도: 4,000m, 보관 고도: 12,000m

안전: IEC/EN 61010-1

유지 관리, 서비스 및 보호 장비 손상

· 사용자가 취급할 수 있는 구성품은 배터리밖에 없습니다. 배터리를 교체하는 경우 외에는 케이스를 열지 마십시오.

· Fluke Networks에서 승인한 교체 부품만 사용하십시오.

· 이 장비를 제조업체가 지정한 방식대로 사용하지 않을 경우 장비의 기본 보호 기능이 제 기능을 못할 수 있습니다.

· 케이스를 청소하려면 물이나 중성 세제와 물 혼합액을 적신 부드러운 천을 사용하십시오.

Fluke Networks 연락처

www.flukenetworks.com

support@flukenetworks.com

+1-425-446-4519

- 오스트레일리아: **61 (2) 8850-3333** 또는 **61 (3) 9329 0244**
- 베이징: **86 (10) 6512-3435**
- 브라질: **11 3759 7600**
- 캐나다: **1-800-363-5853**
- 유럽: **+31-(0) 40 2675 600**
- 홍콩: **852 2721-3228**
- 일본: **03-6714-3117**
- 한국: **82 2 539-6311**
- 싱가포르: **+65-6799-5566**
- 대만: **(886) 2-227-83199**
- 미국: **1-800-283-5853**

전체 전화번호 목록을 확인하려면 당사 웹 사이트를 방문하십시오.

배터리 충전 및 수명

처음 사용하기 전에 배터리를 4시간 충전하십시오. 배터리를 충전하려면 AC 어댑터를 AirCheck 테스터의 배터리 커넥터에 연결하십시오.

배터리 수명은 일반적인 작동 시 약 5.5시간입니다.

배터리 상태를 표시합니다. 배터리가 부족하면 아이콘이 깜박입니다.

AC 어댑터가 연결되었음을 표시합니다.

홈 화면

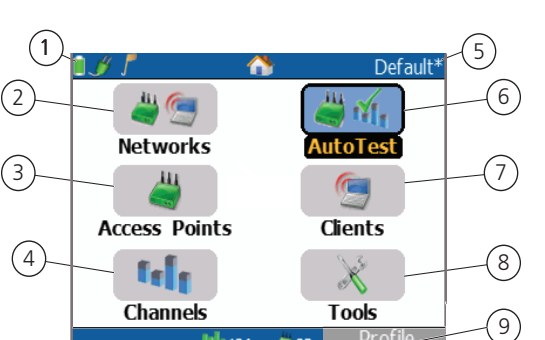


그림 1. 홈 화면 구성 요소

①

배터리 상태를 표시합니다. 배터리가 부족하면 아이콘이 깜박입니다. AC 어댑터를 연결하여 배터리를 충전하고 테스터가 계속 작동하는지 확인하십시오.

AC 어댑터가 연결되었음을 표시합니다.

외부 안테나가 연결되었음을 표시합니다.

참고

외부 안테나가 연결되어 있을 경우 AirCheck은 전송 작업을 진행하지 않으며 액세스 지점에 연결되지 않습니다.

② **Networks(네트워크)**: 무선 LAN을 검색합니다.

③ **Access Points(액세스 지점)**: 액세스 지점을 검색합니다.

④ **Channels(채널)**: 사용 중인 WLAN 채널을 표시합니다.

⑤ 테스터가 현재 사용 중인 프로필 이름. 다른 프로필을 로드하지 않은 경우 이 프로필이 **Default(기본값)**입니다. 프로필을 로드하거나 저장한 이후 테스터의 설정을 변경한 경우 프로필 이름 옆에 별표가 표시됩니다.

⑥ **AutoTest(자동 검사)**: 무선 품질(채널 사용 및 간섭), 네트워크 품질(네트워크 커버리지 및 연결성)과 애드혹 네트워크의 존재를 확인하여 네트워크의 상태를 자동으로 점검합니다. 비인증 액세스 지점 감지는 선택 사항이며 ACL 구성이 필요합니다.

⑦ **Clients(클라이언트)**: 네트워크를 사용하여 클라이언트를 검색합니다.

⑧ **Tools(도구)**: 파일 및 설정을 관리할 수 있습니다.

⑨ **Profile(프로필)**: 사용할 수 있는 프로필 목록을 표시합니다.

⑩ 좌측: 테스터가 현재 모니터링 중인 채널. 막대의 색은 규제 도메인에 대한 국가 코드의 상태를 표시합니다. 빨간색 아이콘은 현재 국가 설정에 대한 불법적인 채널 운영 및/또는 다른 국가 코드의 수신을 나타낼 수 있습니다.

우측: 테스터가 수신하는 물리적 액세스 지점의 수입니다.

최대 **500**개의 액세스 지점이 테스터의 액세스 지점 데이터베이스에 저장될 수 있습니다. 액세스 지점 아이콘이 노란색으로 변하면 **400**개 이상의 액세스 지점이 검색되었음을 나타냅니다.

아이콘이 빨간색으로 변하면 **500**개 이상의 액세스 지점이 검색되었으며 액세스 지점 데이터베이스가 꽉 찼음을 나타냅니다. 새로 검색된 액세스 지점은 목록에 포함되지 않습니다.

최고의 성능을 위한 최소 구성

언어 및 국가 설정을 변경하려면

1 **Tools(도구)**를 선택합니다.

2 화면의 언어를 변경하려면 **Set Language(언어 설정)**를 선택합니다. 원하는 언어를 강조 표시한 다음 F2 **Save(저장)**를 누릅니다.

3 국가를 변경하려면 **Set Country(국가 설정)**를 선택하고 테스터를 사용할 국가를 선택한 다음 F2 **Save(저장)**를 누릅니다.

테스터를 최고의 성능으로 사용하려면 AirCheck™ Manager 소프트웨어를 사용하여 프로필을 구성하고 테스터로 업로드하십시오. 프로필은 AirCheck 테스터에서도 구성할 수 있으며 프로필에는 테스터로 다음과 같은 작업을 수행하기 위한 데이터가 포함됩니다.

- 보안 자격 증명이 필요한 네트워크에 연결
- 각 액세스 지점에 대한 정확한 인증 상태 표시. 이를 통해 어떤 액세스 지점이 네트워크에서 인증된 부분인지 신속히 확인할 수 있습니다.
- 주요 네트워크 장치에 대한 Ping
- 호스트 이름 또는 IP주소와 지정된 포트 번호를 사용하여 TCP 포트 연결 검사 실행

무선 네트워크에서 확인할 수 있는 사항

내 네트워크의 상태는 어떻습니까?

❑ **Wi-Fi 무선 품질은 어떻습니까?**
채널에 액세스 지점과 Wi-Fi 트래픽으로 과부하가 발생하지는 않았습니까?
잡음이 심하게 발생한 채널은 없습니까?

AutoTest(자동 검사)를 선택합니다. 자동 검사를 실행한 후, **Air Quality(무선 품질)**를 선택하여 802.11 채널 사용률, 비-802.11 채널 사용률 및 동일 채널 간섭 상태 평가의 결과를 확인합니다.

802.11 채널 사용률 결과에는 가장 많은 Wi-Fi 트래픽을 갖는 최상위 세 개의 채널이 포함됩니다. 채널 사용률 값은 ✓ 통과, ⚠ 경고 또는 ✗ 실패의 등급과 함께 표시됩니다. 검사 등급은 사용자가 설정할 수 있는 임계값과 실제값을 비교하여 결정됩니다. 이러한 임계값은 **Tools(도구) > Thresholds/AutoTest Settings(임계값/자동 검사 설정)에서 구성할 수 있습니다**.

비-802.11 채널 사용률 결과에는 가장 많은 비-802.11 간섭 및 잡음이 발생한 최상위 세 개의 채널이 포함됩니다. 해당 채널의 사용률 값은 ✓ 통과, ⚠ 경고 또는 ✗ 실패의 등급과 함께 표시됩니다.

동일 채널 간섭 결과에는 최소한의 신호 강도와 신호 품질을 가진 AP 개수가 가장 많은 최상위 세 개의 채널이 포함됩니다. AP 수는 ✓ 통과, ⚠ 경고 또는 ✗ 실패 이상의 등급과 함께 표시됩니다.

- **Wi-Fi 네트워크의 품질은 어떻습니까?**
  내 네트워크를 지원하는 액세스 지점을 수신할 수 있습니까?
  이 영역에 커버리지 홀이 있습니까?
  같은 채널을 사용하는 인접한 AP가 너무 많아 네트워크가 느려지고 있지는 않습니까?
  저도 접속할 수 있습니까?

  AutoTest(자동 검사)를 선택합니다- 자동 검사를 실행한 후, **Network Quality(네트워크 품질)**를 선택하여 커버리지, 동일 채널 간섭, 보안 및 연결 상태 평가의 결과를 확인합니다.

  커버리지 결과에는 네트워크(SSID)를 지원하는 좋은 신호 강도와 좋은 신호 대 잡음비를 갖는 AP의 수와 ✓통과, ⚠ 경고 또는 ✗ 실패의 등급이 표시됩니다. 검사 등급은 사용자가 설정할 수 있는 임계값과 실제값을 비교하여 결정됩니다. AP 수 및 신호 수준과 신호 대 잡음비의 신호 품질 임계값은 **Tools(도구) > Thresholds/AutoTest Settings(임계값/자동 검사 설정) > AP Coverage(신호 커버리지), Signal level(신호 수준)** 및 **Signal-to-noise Threshold**(신호 대 잡음비 임계값) 화면에서 설정할 수 있습니다.

  동일 채널 간섭 결과에는 네트워크의 중복 AP의 수가 임계값에 대비한 단일 네트워크의 비교를 기반으로 ✓통과, ⚠ 경고 또는 ✗ 실패의 등급과 함께 포함됩니다. 이 검사의 임계값은 **Tools(도구) > Thresholds/AutoTest Settings(임계값/자동 검사 설정) > Network Quality co-channel thresholds(네트워크 품질 동일 채널 임계값)** 화면에서 설정할 수 있습니다.

보안 결과에서는 SSID의 모든 AP가 동일한 보안 자격 증명을 사용하는지 여부를 ✓ 통과, ⚠ 경고 또는 ✗ 실패의 등급과 함께 보고합니다.

연결 검사는 프로필에 구성된 각 네트워크에 연결을 시도합니다. 연결 검사 결과는 현재 위치에서 네트워크로의 연결이 가능한지 그렇지 않은지를 통과 또는 실패의 검사 등급으로 표시합니다. 연결과 관련한 추가 세부 정보(예: 채널, 수신된 IP 주소와 연결 속도)가 ✓ 통과, ⚠ 경고 또는 ✗ 실패의 등급으로 제공됩니다.

❑ **어떤 인증되지 않았거나 알 수 없는 액세스 지점이 Wi-Fi 네트워크에 연결되어 있습니까? 이러한 지점에는 보안 위험이 있습니까?**

비인증 액세스 지점 검사는 자동 검사의 선택사항으로, 인증되지 않았거나 알 수 없는 액세스 지점의 감지 여부를 ✓ 통과, ⚠ 경고 또는 ✗ 실패의 등급으로 표시합니다. 결과에는 사용자의 위치에서 수신되는 모든 비인증 액세스 지점이 포함됩니다. 비인증 액세스 지점을 식별하려면 액세스 제어 목록(ACL)을 구성해야 합니다. ACL 구성은 자동 검사 화면에서 **Rogue Access Points(비인증 액세스 지점) > ACL** 또는 **Home(홈)> Access Points(액세스 지점) > ACL**을 선택하여 설정할 수 있습니다.

무선 LAN에는 어떤 것이 있습니까?

❑ **어떤 무선 LAN을 사용할 수 있습니까?**

Networks(네트워크)를 선택하여 무선 LAN과 각 네트워크에 연결된 액세스 지점의 목록을 확인할 수 있습니다. 사용자의 위치에서 사용 가능한 모든 액세스 지점을 보려면 **Access Points(액세스 지점)**를 선택합니다.

❑ **어떤 액세스 지점을 사용할 수 있습니까? 신호 강도는 충분합니까?**

Access Points(액세스 지점)를 선택하여 사용자의 위치에서 사용 가능한 액세스 지점과 해당 액세스 지점의 신호 강도의 목록을 확인할 수 있습니다. 특정 액세스 지점의 신호 강도 및 잡음에 대한 막대 그래프를 보려면 액세스 지점을 강조 표시한 다음 SELECT을 누릅니다.

❑ **액세스 지점이 올바르게 구성되었습니까?**

홈 화면에서 **Access Points(액세스 지점)**를 선택하고 액세스 지점을 강조 표시한 다음 SELECT을 누릅니다.

❑ **해당 영역에 새로운 액세스 지점이 있습니까? 새 지점은 사용자의 액세스 지점입니까, 아니면 인접 사용자 또는 비인증 액세스 지점입니까?**

장치 인증 상태(ACL) 기능을 사용하여 사용자의 위치에서 검색된 새로운 액세스 지점을 자동으로 보고할 수 있습니다. 이 기능을 사용하려면 각 액세스 지점(예: 인증된 지점 또는 인접 지점)의 액세스 지점 인증 상태를 구성하고 기본 인증 상태를 **? Unknown(알 수 없음)**으로 설정합니다. 그러면 **? Unknown(알 수 없음)**의 기본 인증 상태가 이전에 발견되지 않은 모든 액세스 지점에 할당됩니다. 마지막으로, 홈 화면에서 홈 화면에서 **Access Points(액세스 지점)**을 선택하여 **? Unknown(알 수 없음)**으로 표시된 모든 액세스 지점을 확인합니다.

또는, 검색된 액세스 지점 목록을 포함하는 검사 세션을 저장합니다. 액세스 지점이 추가로 검색되었는지 확인하려면 AirCheck Manager를 사용하여 이전에 저장된 세션 파일과 액세스 지점 목록을 비교합니다.

기본 장치 인증을 알 수 없음 또는 인증됨으로 지정하려면 **Tools(도구) > Set Device Authorization (ACL) default(장치 인증(ACL) 기본값 설정)**를 선택합니다.

❑ **어떤 무선 클라이언트가 네트워크를 사용합니까?**

홈 화면에서 **Clients(클라이언트)**를 선택합니다. 연결된 클라이언트 목록을 보려면 AP 또는 채널 세부 정보를 확인해도 됩니다.

장치를 무선 네트워크에 연결할 수 있습니까?

테스터를 사용하여 연결성을 확인합니다.

- ❑ **장치가 클라이언트로서 네트워크(SSID)에 연결할 수 있습니까?**

  Networks(네트워크)를 선택하고 네트워크를 강조 표시한 다음 F1 **Connect(연결)**를 누릅니다.

  참고

  보안 네트워크에 연결하려면 테스터에 보안 자격 증명이 포함된 프로필이 있어야 합니다.

- ❑ **장치를 액세스 지점(BSSID)에 연결할 수 있습니까?**

  Access Points(액세스 지점)를 선택하고 액세스 지점을 강조 표시한 다음 F1 **Connect(연결)**를 누릅니다. **Connect(연결)**의 오른쪽에 *가 있는 경우 이는 테스터에 해당 네트워크에 대한 보안이 구성되지 않았음을 나타냅니다. **Connect*(연결)**를 누르면 보안 설정 입력으로 진행됩니다. 입력이 마무리되면 보안 설정이 편재 프로필에 저장됩니다. 필요한 경우 **Tools(도구)**를 누른 다음 **Manage profiles(프로필 관리) / network passwords(네트워크 암호)**를 눌러 보안 설정을 다시 편집합니다.

- ❑ **장치가 네트워크 또는 액세스 지점에 연결할 수 없는 경우, 연결 절차가 실패한 곳은 어디입니까?**

  연결 로그를 확인합니다. **Connect to Network(네트워크에 연결)** 또는 **Connect to Access Point(액세스 지점에 연결)** 화면에서 F2 **Log**(로그)를 누릅니다.

❑ **장치가 네트워크 장치로 Ping을 수행할 수 있습니까?**

Ping 검사를 수행합니다. 네트워크 또는 액세스 지점에 연결한 다음 F1 **Start tests**(검사 시작)를 누릅니다.

참고

Ping 대상은 ***Tools(도구) > Manage profiles (프로필 관리) / network passwords(네트워크 암호) > Edit targets(대상 편집) > Add(추가)****를 선택하여 추가할 수 있습니다. IP 주소 또는 호스트 이름(URL)으로 대상을 추가할 수도 있습니다.*

Connect(연결)*의 오른쪽에* ******* *가 있는 경우 이는 테스터에 해당 네트워크에 대한 보안이 구성되지 않았음을 나타냅니다.* ***Connect*(연결)****를 누르면 보안 설정 입력으로 진행됩니다.*

❑ **클라이언트의 네트워크 인터페이스 카드가 정상적으로 작동합니까?**

Clients(클라이언트)를 선택하고 SSID 열을 확인합니다. 대시 표시된 SSID는 클라이언트를 프로빙하고 있으며 SSID 이름이 표시된 클라이언트는 연결 클라이언트입니다. SELECT을 눌러 클라이언트가 프로브 요청 프레임을 전송할 수 있는지 확인합니다.

네트워크 성능 저하 또는 연결 중단의 원인이 무엇입니까?

❑ **신호 강도가 충분합니까?**

Access Points(액세스 지점)를 선택합니다. **Access Points(액세스 지점)** 화면에 각 액세스 지점의 신호 강도가 표시됩니다. 액세스 지점을 선택하여 신호 강도 및 정체에 대한 세부 정보를 확인합니다.

❑ **네트워크 사용량이 많습니까?**

Channels(채널)을 선택하여 채널 사용과 각 채널을 사용하는 액세스 지점 수에 대한 개요를 확인합니다. 그래프를 보려면 채널을 강조 표시한 다음 SELECT를 누릅니다.

❑ **채널에 비-802.11 인터페이스가 있습니까?**

Channels(채널)을 선택합니다. 비-802.11 인터페이스가 회색으로 표시됩니다. 이 잡음이 WLAN 연결 또는 성능에 간섭을 일으킬 수 있습니다. 비-802.11 잡음은 전자레인지, 무선 전화기, Bluetooth® 장치, 동작 탐지기, 무선 카메라 및 기타 무선 장치에서 발생할 수 있습니다.

참고

위의 세 가지 측정은 ***AutoTest(자동 검사)*** *기능에도 요약되어 있습니다.*

네트워크에 보안 위험이 있습니까?

❑ **네트워크가 예상 보안 수준으로 운영됩니까?**

Networks(네트워크)를 선택합니다. 보안되지 않은 액세스 지점이 있는 네트워크에 빨간색 자물쇠()가 표시됩니다.

❑ **해당 영역에 애드혹 네트워크가 있습니까?**

Networks(네트워크)를 선택합니다. 애드혹 네트워크 모드에서 작동하는 스테이션은 **SSID** 열에 애드혹 아이콘()으로 표시됩니다. 애드혹 스테이션은 네트워크 보안 위험을 초래하거나 네트워크 정책을 위반할 수 있습니다.

자동 검사에는 애드혹 스테이션을 표시하는 애드혹 네트워크 검사가 포함됩니다.

❑ **해당 영역에 비인증 액세스 지점이 있습니까? 어디에 있습니까?**

AirCheck을 사용하여 검색된 액세스 지점의 인증 상태를 추적할 수 있습니다. 기본적으로 액세스 지점이 검색되면 검색된 액세스 지점의 인증 상태는 ? **Unknown(알 수 없음)**으로 할당됩니다. 사용자 네트워크에 대한 관계(예, 인증됨, 인접, 인증되지 않음)를 적용하기 위해 개별 또는 그룹 액세스 지점의 상태를 변경할 수 있습니다.

또한 기본 장치 상태를 ? **Unknown(알 수 없음)**에서 ✓ **Authorized(인증됨)**로 변경할 수 있습니다. 변경이 완료되면 검색된 모든 액세스 지점은 ✓ **Authorized(인증됨)**로 확인됩니다. 그러면 사용자는 목록을 검토하여 개별 액세스 지점에 해당하는 상태를 할당할 수 있습니다. 예를 들어, 사용자가 특정 액세스 지점이 비인증 상태임을 알고 있는 경우 해당 지점에 **플래그 표시된 장치** 또는 ⚠ **인증되지 않은 장치** 상태를 부여할 수 있습니다.

기본 장치 인증을 지정하려면 **Tools(도구) > Set Device Authorization (ACL) default(장치 인증 (ACL) 기본값 설정)**를 선택합니다.

개별 또는 그룹 액세스 지점에 인증 상태를 지정하려면 **Access Points(액세스 지점)**를 선택하고 액세스 지점을 강조 표시한 다음 F2 **ACL**을 누릅니다.

✓ **Set All APs to Authorized(모든 AP를 인증됨으로 설정)**를 선택하여 모든 액세스 지점의 인증 상태를 ✓ **Authorized(인증됨)**로 설정할 수 있습니다. 그러면 검색된 모든 액세스 지점이 ✓ **Authorized (인증됨)**로 표시됩니다. 이 방법을 사용하면 기본 인증 상태가 ? **Unknown(알 수 없음)**으로 설정되어 있을 경우 새로 검색된 액세스 지점은 ? **Unknown (알 수 없음)**으로 표시됩니다. 일반적으로 이 방법을 사용하면 보안 위험이나 새로운 액세스 지점을 신속하게 확인할 수 있습니다.

또한, 사용자는 ✓ **Set AP series to Authorized(AP 시리즈를 인증됨으로 설정)**또는 ⚠ **Set AP series to Unauthorized(AP 시리즈를 인증되지 않음으로 설정)**를 선택하여 일련의 AP를 AP BSSID/MAC 또는 공급업체 MAC 접두어를 기준으로 인증됨 또는 인증되지 않음으로 설정할 수 있습니다. 이 옵션은 구성에 필요한 시간을 절약하고 잠재적 문제를 신속하게 확인할 수 있도록 지원합니다. 예를 들어, 특정 공급업체의 장비가 네트워크 정책에 따라 허용되지 않는 경우, 공급업체 MAC 접두어를 사용하여 ACL을 인증되지 않음으로 설정할 수 있습니다. 이러한 액세스 지점이 감지되면 해당 액세스 지점은 인증되지 않음으로 자동 보고됩니다.

참고

사용자가 프로필을 저장하면 할당된 ACL 역시 프로필의 일부로 저장됩니다.

자동 검사에는 비인증 액세스 지점을 감지하여 보고하는 비인증 액세스 지점 검사가 선택적으로 포함됩니다. 이 기능을 사용하려면 **Tools(도구) > Thresholds/AutoTest Settings(임계값/자동 검사 설정) > Rogue Access Point AutoTest(비인증 액세스 지점 자동 검사)**로 이동합니다. 정확하고 의미 있는 검사 결과를 얻으려면 자동 검사를 실행하기에 앞서 액세스 지점 ACL을 구성해야 합니다.

액세스 지점을 어떻게 찾을 수 있습니까?

Access Points(액세스 지점)를 선택하고 액세스 지점을 하나 선택한 다음 **Access Point Details(액세스 지점 세부 정보)** 화면에서 F2 **Locate(찾기)**를 누릅니다. 옵션으로 제공되는 Fluke Networks 외부 지향성 안테나를 사용하면 액세스 지점을 보다 빨리 찾을 수 있습니다.

내 네트워크 및 내 검사 세션을 어떻게 문서로 만들 수 있습니까?

을 눌러 세션을 저장한 다음 AirCheck Manager 소프트웨어를 사용하여 데이터를 PC로 다운로드하고 보고서를 만들 수 있습니다.

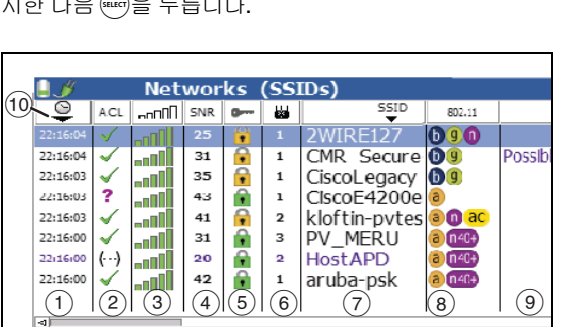
어떻게 하면 AirCheck의 모든 정보를 지울 수 있습니까?

모든 설정과 세션 데이터 및 프로필을 테스터에서 지우려면 **Tools(도구) > Erase All(모두 지우기)**을 선택합니다. AirCheck 테스터에 저장된 모든 정보가 삭제됩니다.

채널, 네트워크, AP 또는 클라이언트 검색

채널, 네트워크, 액세스 지점 또는 클라이언트를 검색하려면 홈 화면에서 **Channels(채널)**, **Networks(네트워크)**, **Access Points(액세스 지점)** 또는 **Clients(클라이언트)**를 선택합니다. 그림 2는 **Networks(네트워크)** 목록을 보여줍니다.

네트워크 또는 액세스 지점에 대한 세부 정보를 보려면 ▲▼를 사용하여 네트워크 또는 액세스 지점을 강조 표시한 다음 SELECT을 누릅니다.



gdp03a.eps

그림 2. 네트워크 목록

① : 테스터가 네트워크로부터 처음 수신한 시간입니다. 사용자가 영역 내에서 이동함에 따라 범위 안으로 포함되는 네트워크를 보려면 타임스탬프 열의 목록을 내림차순으로 정렬합니다.

을 누른 다음 영역 내에서 이동합니다. 범위 안으로 포함되는 네트워크가 목록의 상단에 추가됩니다. **Gray inaudible access points(수신할 수 없는 액세스 지점 회색 표시)**를 사용하는 경우, 범위를 벗어나는 네트워크가 회색으로 표시됩니다.

② **ACL**: 액세스 지점의 인증 상태입니다. 기본 상태는 **? Unknown(알 수 없음)**이지만, **✓ Authorized (인증됨)**로 변경할 수 있습니다. 사용자 네트워크와 관련되는 방식을 표시하려면 각 액세스 지점의 상태를 변경합니다. 상태를 변경하려면 홈 화면에서 **Access Points(액세스 지점)**를 선택하고 액세스 지점을 하나 선택한 다음 F2 **ACL**을 누릅니다.

(...): 네트워크의 모든 액세스 지점이 동일한 인증 상태는 아닙니다.

③ : 특정 네트워크 SSID에 대한 모든 액세스 지점의 최대 신호 강도입니다.

④ **SNR**: 신호 대비 잡음비는 잡음에 대한 상대적 신호 강도를 나타내는 측정값입니다. 이 비율은 데시벨(dB)로 측정됩니다.

⑤ : 네트워크의 보안 상태입니다.

빨간색 열린 자물쇠: 네트워크에 대해 보안이 사용되지 않습니다.

참고

잠금이 해제된 일부 네트워크에서는 사용자가 테스터를 연결하거나 Ping 검사 실행을 비롯한 측정을 할 수 있지만, 같은 네트워크에 연결된 PC가 사용자 ID와 암호 없이 웹에 연결하는 것은 허용되지 않을 수 있습니다.

노란색 잠긴 자물쇠: 하나 이상의 액세스 지점에서 WEP 또는 Cisco LEAP 보안 프로토콜을 사용합니다. 이는 다른 프로토콜에 비해 안전 수준이 낮습니다.

녹색 잠긴 자물쇠: 모든 액세스 지점이 WEP보다 안전한 보안 프로토콜(예: WPA 또는 WPA2)을 사용합니다.

(...): 네트워크의 모든 액세스 지점이 동일한 보안 유형을 사용하지는 않습니다. 예를 들어, 어떤 액세스 지점은 WEP를 사용하고 다른 액세스 지점은 WPA를 사용할 수 있습니다.

⑥ : 사용자의 위치에서 테스터가 수신하는 액세스 지점의 수입니다.

⑦ **SSID**: 서비스 집합 ID(Service Set Identifier). 무선 네트워크의 이름입니다.

: 네트워크에 애드혹 장치가 있습니다. 이는 액세스 지점을 거치지 않고 다른 장치와 직접 통신하는 장치를 말합니다. 애드혹 장치를 통해 해커가 네트워크에서 전송되는 데이터에 액세스할 수 있습니다(일부 네트워크 IT 정책은 애드혹 장치를 허용함).

[Hidden(숨김)]: SSID를 브로드캐스트하지 않는 네트워크입니다.

⑧ **802.11**: 네트워크의 액세스 지점이 사용하는 802.11 표준입니다.

802.11a: 5GHz 대역을 사용합니다.

802.11b: 2.4GHz 대역을 사용합니다.

802.11g: 2.4GHz 대역을 사용합니다.

802.11n: 2.4GHz 또는 5GHz 대역을 사용합니다.

ac 802.11ac: 5GHz 대역을 사용합니다.

빨간색 막대: 빨간색 막대: 테스터가 **Tools(도구) > Set country(국가 설정)**의 설정과 다른 국가 코드를 수신했습니다. 해당 코드를 전송하는 네트워크 또는 액세스 지점을 식별하려면 **Networks(네트워크)** 또는 **Access Points(액세스 지점)**를 선택한 다음 **802.11**열에서 빨간색 막대를 찾습니다.

n40+ n40–: 하나 이상의 액세스 지점이 결합된 채널을 사용합니다. 802.11n 표준을 사용하는 액세스 지점은 하나의 40MHz 채널을 만들기 위해 채널과 상위(n40+) 또는 하위(n40–)의 확장 채널을 결합할 수 있습니다. 이러한 광범위한 채널을 통해 네트워크 처리량이 확대됩니다.

(...): 네트워크의 모든 액세스 지점이 동일한 802.11 표준을 사용하지는 않습니다.

⑨ **Notes(노트)**: 노트 필드로 스크롤 하려면 ▸을 누릅니다. 테스터가 자동으로 노트를 추가합니다. 노트가 있는 네트워크는 자주색으로 표시됩니다.

(...): 네트워크에 여러 노트가 있습니다. 모든 노트를 보려면 네트워크를 강조 표시한 다음 SELECT을 두 번 눌러 **Access Point Details(액세스 지점 세부 정보)** 화면으로 이동합니다.

⑩ ▼▲: **Sort 1(정렬 1)**, 내림차순 또는 오름차순

▼ ▲ : **Sort 2(정렬 2)**, 내림차순 또는 오름차순

목록을 오름차순 또는 내림차순으로 정렬하려면 ▲▼ 및 ◀▶을 사용하여 열 머리글을 강조 표시한 다음 SELECT 또는 F1 **Sort 1(정렬 1)**을 누릅니다. 예를 들어, 신호가 가장 강한 액세스 지점을 신속히 찾으려면 열 상단의 ▁▂▃▅▇을 강조 표시한 다음 SELECT 또는 F1 **Sort 1(정렬 1)**을 누릅니다. 이렇게 하면 신호가 가장 강한 액세스 지점이 목록의 상단에 표시됩니다.

두 번째 순서로 정렬하려면 다른 열 머리글을 강조 표시한 다음 F2 **Sort 2(정렬 2)**를 누릅니다.

⑪ 강조 표시된 네트워크에 연결하려면 F1 **Connect (연결)**를 누릅니다.

테스터가 강조 표시된 네트워크에 연결할 수 없는 경우 연결 버튼이 **Connect*(연결*)**(별표와 함께 표시)로 표시됩니다. 네트워크의 보안 설정을 구성하려면 F1 **Connect*(연결*)**를 누릅니다.

참고

보안 네트워크에 연결하려면 테스터에 보안 자격 증명이 포함된 프로필이 있어야 합니다. 테스터에서 또는 AirCheck Manager를 사용하여 보안 자격 증명을 생성하거나 편집할 수 있습니다. 테스터의 ***Connect*(연결*)****를 누르면 보안 구성으로 연결됩니다.* ***Tools(도구)****를 누른 다음* ***Manage profiles(프로필 관리) | network passwords (네트워크 암호)****를 눌러 보안 설정을 재구성할 수 있습니다.* ***Connect(연결)****의 오른쪽에 *** *가 있는 경우 이는 보안 설정이 구성되지 않았음을 나타냅니다. 연결을 사용하여 보안 절차를 설정하려면 사용 설명서를 참조하십시오.*

⑫ 40: 테스터가 현재 모니터링하는 채널입니다. 막대의 색은 규제 도메인에 대한 국가 코드의 상태를 표시합니다.

⑬ : 사용자의 위치에서 테스터가 수신하는 액세스 지점의 수입니다. **Group virtual access points (가상 액세스 지점 그룹화)**가 선택된 경우 이 수에 가상 액세스 지점은 포함되지 않습니다.

⑭ **Networks(네트워크)** 화면의 아이콘에 대한 설명을 보려면 F2 **Legend(범례)**를 누릅니다.

네트워크의 액세스 지점에 대한 세부 정보를 보려면 ◁▷을 사용하여 네트워크를 강조 표시한 다음 SELECT를 누릅니다.